

www.hacker-journal.com

2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS

LINUX
Primeros pasos para instalarlo

IRC
Un territorio por explorar

TROYANOS
...Y te infecto un archivo

Seguridad en el éter
Seguridad en el protocolo 802-11b

RICHARD STALLMAN



Profeta del software libre

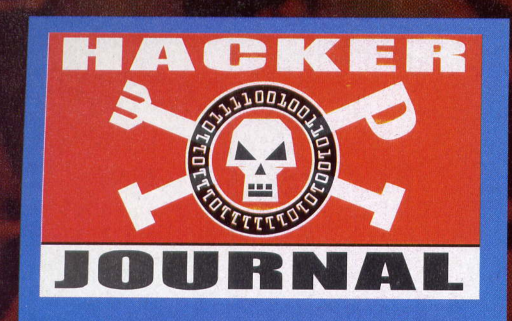
Palladium
El Gran Hermano ataca de nuevo

N. 4



4ever

>>> PRÁCTICA >>> SEGURIDAD >> MAC >>> LINKS



Año 2 - N. 4
Enero-Febrero 2004

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Infoambiente, Ana Esteban, Gualtiero Tronconi, Eduardo Bracaglia

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ǝr)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

PRIVACIDAD Y SEGURIDAD

Los hechos del 11 de septiembre configuraron un panorama sin precedentes. Todos aquellos que estaban esperando su oportunidad para lanzarse sobre las libertades individuales encontraron abiertas las puertas para lanzarse de cabeza a defender sus propuestas y, de paso, hacer negocio. Negocio redondo.

Una de las características de Internet es y ha sido el anonimato. Gracias a este anonimato, uno podía pasear por la red con la misma tranquilidad que podría estar mirando escaparates en una calle concurrida. Desafortunadamente, más de uno se ha aprovechado de este anonimato para cometer excesos o agredir la libertad de los demás. Es el caso, por ejemplo, del correo spam o de la difusión de virus. Es legítimo y necesario buscar soluciones ante estos excesos, pero cuando se compromete la privacidad, las cosas se complican inmediatamente.

En el número que tenéis entre manos encontraréis un reportaje sobre Palladium, una propuesta encabezada por Microsoft e Intel para promover una informática personal basada en claves cifradas... que deja fuera del juego al propio usuario. Bajo la cobertura de certificar la seguridad y la estabilidad del ordenador, lo que se pretende es dar un zarpazo a la libertad individual para coneguir que paguemos por todo, que sólo hagamos lo que se nos diga que podemos hacer, que no hagamos copias de seguridad a pesar de que la legislación nos garantice este derecho... El problema es tan viejo como el mundo: ¿quién vigila al vigilante? Si no aclaramos esta cuestión, el liberalismo radical tiene sus propios planes para conseguir sacar todo el jugo a cada usuario. El principio es sencillo: el pez grande se come al chico. ¿Eres más pequeño que Microsoft, que Intel, que Yahoo o que tantos otros? Pues nada, a ser digerido. No parece justo, ¿verdad? Pues será mejor que no nos durmamos con cantos de sirenas, y que nos esforcemos por ver qué se esconde tras cada propuesta.

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS

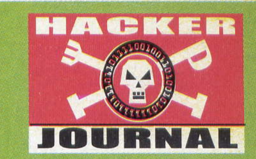

NEWBIE


MID HACKING


HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

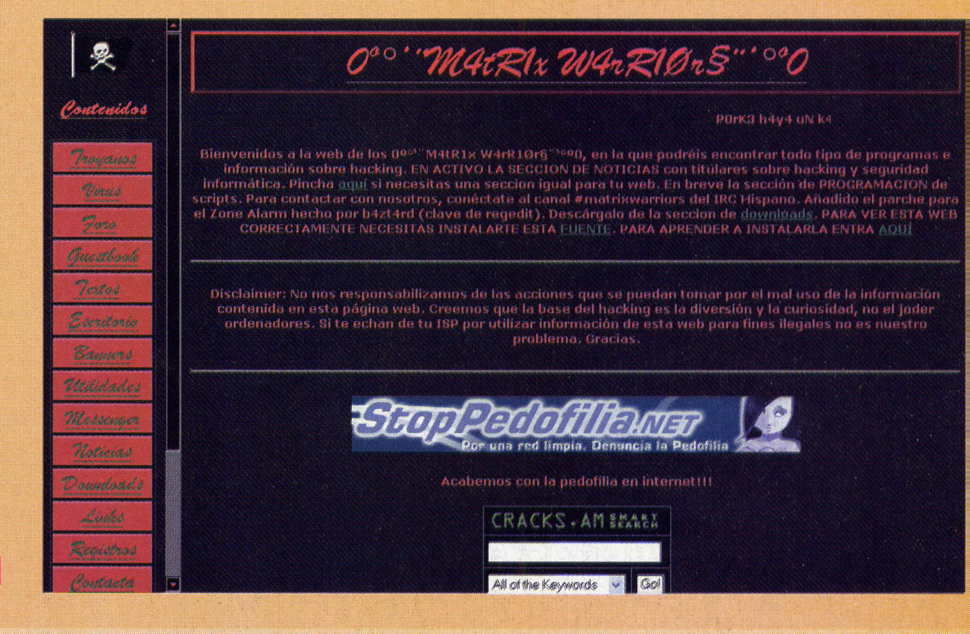
Número 4 - Enero - Febrero 2004



SITIO WEB

Buenas. Ante todo felicidades por ese pedazo de revista que os habeis currao, se nota que está trabajadísima. Bueno, me gustaría que mi web apareciese reseñada en vuestra revista. Es de un grupillo de hacking bastante modesto, pero procuramos aprender cada día más, y esto se consigue en parte gracias a vuestra revista. xD, bueno, la direccion es www.matrixwarriors.cjb.net. Gracias de antemano.

b4zt4rd

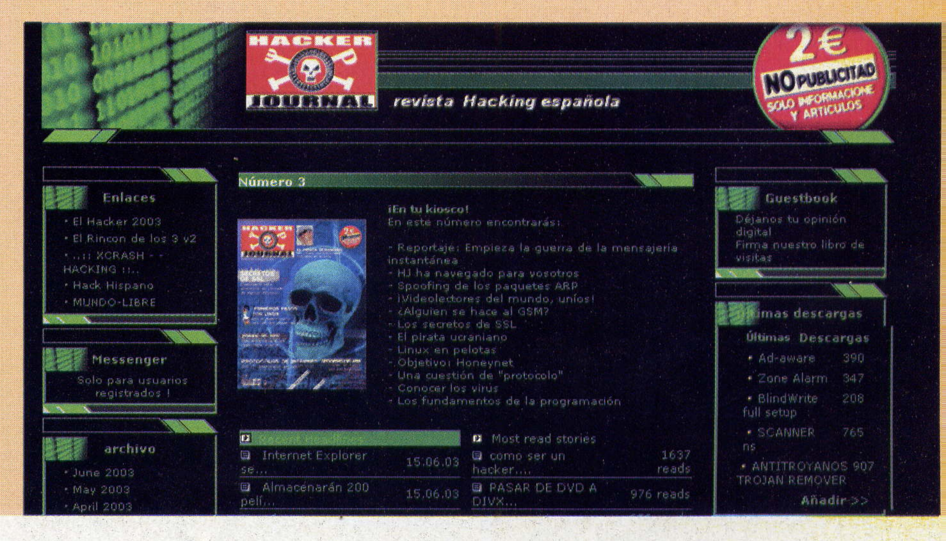


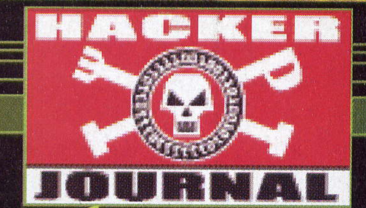
Visita nuestro sitio web:
www.hacker-journal.com

¡SECRET ZONE!

He aquí los códigos para acceder a la Secret Zone de nuestro sitio, donde podréis encontrar información y utilidades interesantes. Con algunos navegadores, puede ser necesario insertar dos veces los mismos códigos. No os detengáis al primer intento

user: secre4
password: estudi0





SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS

mailto:

redaccion@hacker-journal.com

VAMOS A ENTENDERNOS

¿Cómo se puede hacer un virus que no requiera mucho tiempo y que sea muy fuerte?

Coran D.S.

Es posible que se nos haya pasado por alto algún detalle, incluso es posible que hablemos idiomas distintos. Pero ha llegado el momento de aclarar esto definitivamente: ¡NO tenemos ninguna simpatía por los virus!

Los virus son perjudiciales, hacen perder montones de tiempo y dinero a todos. Los más perjudicados son aquellos que tienen menos conocimientos, para quienes de pronto el ordenador se convierte en un trasto que hace lo que le parece de forma incomprensible, mientras alguien espía su intimidad o le destruye su trabajo. ¿De verdad quieres construir virus demoledores? Pues busca en otro sitio. Aquí no nos dedicamos a eso. Muy al contrario, luchamos por divulgar la información necesaria para que todos podamos protegernos de excesos como el que tú querrías perpetrar. Si de verdad quieres ser un hacker, aprende y aprende para mejorar la seguridad de todos, y deja este mundo mejor de como lo encontraste al llegar.

EL GUSTO ES NUESTRO

Hola,
Estoy encantado con su revista, encontré el nº 1 por casualidad y desde entonces vigilo el kiosko para que no se me escape ni una, es por eso que envío este mail, a ver si se animan y ponen la suscripción, a mi ya me tienen como cliente de seguro, tambien felicitarles por la web, no es que esté muy movida pero según se enganchen gente a la revista esto va a ser la leche.

http://www.kioscoinformatico.com/

Kioscoinformatico.com

Revistas	Pedidos	Diario de Salidas	Enlaces	Servicio de Avisos

	En esta sección podéis consultar los titulares e imagen de portada de las revistas de informática del mercado	@	Podéis daros de alta gratuitamente en este Servicio de Avisos y os avisaremos el día que salgan las revistas que elijais.
NUEVO	En este nuevo Diario de Salidas se pueden visitar los números atrasados y se ha paginado hacia atrás para ir buscando lo que os interesa.	Pedidos	Al seleccionar el número de revistas y el título, se mostrará el importe del pedido mediante todas las formas de entrega, al validarlo se pasa a rellenar los datos del pedido en firme.
Enlaces	En la sección de Enlaces acojemos las webs relacionadas con los temas de revistas que tratamos y algunos más siempre relacionados con la informática.	QUIENES SOMOS	Somos un punto de venta de Madrid que tratamos de ofrecer toda la información posible sobre las revistas de informática en general y la posibilidad de conseguirlas.
	Próximamente colocaremos un foro para que consultéis entre vosotros opiniones y consultas sobre las revistas.		Estamos preparando un buscador de articulos por palabras que os será de grán ayuda a la hora de buscar algo concreto.

KIOSCOINFORMATICO.COM : C/ Princesa, 82 - Madrid - TELÉFONO : 659-05-62-59 / E-MAIL - info@kioscoinformatico.com

TITULAR - Paloma Fernández / NIF - 01185304E - WEBMASTER - Carlos Fernández

Con repecto a los artículos me gustaría pedir alguno a ver si hay suerte, uno de ellos podría ser:" qué es un troyano o un gusano o un virus etc.. y en qué se diferencian, qué buscan sus creadores", "creación de un servidor y su seguridad" sobre esto sí he visto algún artículo pero casi se me funden las neuronas, creo que se llama ataque a un servidor sql o así... Bueno de nuevo felicidades

Prisco C.

Muchas gracias por la cálida acogida. El tema de la suscripción nos preocupa y estamos trabajando en ello, pero de momento no podemos decir más.

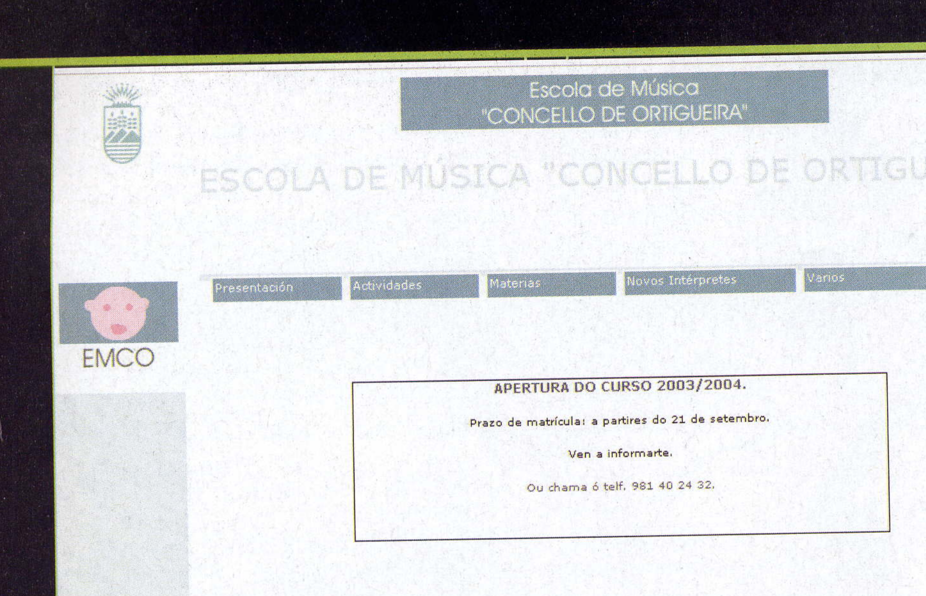
Respecto de los artículos que pides, como irás viendo en los distintos números de Hacker Journal son precisamente los temas que nos interesan también a nosotros. Este mes, en las páginas 26 y 27 encontrarás un nuevo artículo sobre las interioridades de los virus. Sobre qué buscan los creadores de virus, sería hablar y no acabar. Se ha dicho de todo, desde que buscan fama hasta que son simples gamberradas, pasando por oscuros intereses económicos... ¡Tal vez un día publiquemos un artículo recogiendo todas las explicaciones!

Finalmente, montar un servidor no es nada trivial, pero es posible. Para ello te irá bien conocer los múltiples aspectos de seguridad involucrados, como la protección contra ataques, el uso de protocolos, abrir y cerrar puertos, y un largo etcétera. Si de verdad quieres montarte un servidor, busca la información necesaria en el Web. Aquí sólo tenemos espacio para hablar de aspectos concretos de seguridad.

PUNTO DE VENTA

Saludos y enhorabuena por vuestra revista.
Tengo un punto de venta en el que como buen aficionado a la informática y consciente de que muchos puntos de venta parece hasta que les asusta este tipo de revistas, yo les doy un exposición preferente. Por otra parte, tengo una web, www.kioscoinformatico.com, en la que expongo las revistas de informatica y pongo sus titulares e imagen desde el mismo día que salen a la venta, para que la gente pueda consultarlo, una compañera vuestra que no me acuerdo su nombre me escribió un mail agradeciéndome que colocara un enlace con vuestra web, ahora os escribo por-





que necesito que me pongais en contacto con alguien de vuestra revista para poder comprar unos cuantos ejemplares del número 1 y del 2, espero que podáis ayudarme ya que tengo clientes esperando.
Un saludo,

Carlos F.
www.kioscoinformatico.com

Nos satisface enormemente que tengas en cuenta nuestra revista y la integres en tu oferta. En contrapartida, desde aquí hemos publicado tu dirección para que más gente la conozca; ¡así tú ganas en visitas y nosotros en venta!
En la página 2 puedes encontrar el staff de la revista, donde se detalla quiénes somos y donde puedes encontrarnos. Para la solicitud de ejemplares para su venta, deberías dirigirte a nuestra distribuidora, Coedis, que es la empresa responsable de estas tareas. Desafortunadamente, ahora mismo no tenemos la posibilidad de servir números anteriores. En cuanto podamos prestar este servicio, lo comunicaremos puntualmente en nuestras páginas.

MÚSICA PARA TODOS

Agradecería que incluyesen la siguiente página web en los buscadores más importantes:
www.concellodeortigueira.com/escolademusica
Muchas gracias

O_trebello

Lo único que está en nuestras manos es publicar el sitio web que nos indicas aquí. Para insertar la página en los principales buscadores de Internet, deberás visitar cada uno de ellos. Los más importantes suelen contar con medios para que los usuarios puedan dar de alta páginas en sus bases de datos. Debido a que cada buscador tiene su propio método, tendrás que iniciar una ronda de visitas.

PANTALLA AZUL

Muy buenas :
Me dijo a vosotros para pediros ke me digais o me ayudeis a conseguir el nº 2 de vuestra revista , ya ke he estado de vacaciones y en el kiosko donde compre el nº 1 ,no me lo han guardado y por lo visto no me lo pueden agenciar ¿me podeis hacer ese favor ¡¡¡¡¡¡¡ ? os lo agradezco un monton , compré el 3º esta semana
Por cierto ¿podeis en algún nº dedicar un par de hojas a esos errores de windows ke se pone todo el monitor azul (error de windows grave de sistema).
En fin, vosotros mismos, seguiré leyendo lo ke editeis
salu2 cordiales

José Ángel E.

Como hemos comentado anteriormente, desafortunadamente no contamos con un servicio de venta de números anteriores. En cuanto podamos ofreceros este servicio, os lo comunicaremos puntualmente.
Respecto al monitor azul, se trata de la conocida "pantalla azul de la muerte", un recurso que Windows utiliza cuando todo ha ido realmente mal. Las causas pueden ser tan variadas que es imposible generalizar. Puede deberse a una aplicación que se ha comportado realmente mal, pero también puede ser debido a una tarjeta de vídeo que hace un mal contacto, a un disco duro en mal estado... Hay que reconocer que en las últimas versiones de Windows, estas pantallas azules se han ido haciendo menos frecuentes, pero aún es posible encontrar alguna...

HACKHISPANO

Hola, soy LUK, webmaster de hackhispano.com, queria agradeceros el haber puesto a HACKHiSPANO en la sección de "HJ ha navegado con vosotros..." del HJ de octubre.
Gracias y seguid así.
PD: dentro de poco saldrá a la red la nueva versión de hackhispano, así que os tendré al dia :P
Un saludo

LUK

Fue un placer insertar vuestro magnífico sitio web. Ahora, publicando tu mensaje, dejamos avisados a los lectores para que sepan que se avecinan cambios. Será cuestión de estar alerta. No resulta fácil encontrar sitios web de calidad como el vuestro, de modo que desde aquí queremos animar a todos aquellos que os dedicáis a divulgar vuestros conocimientos para que todos se puedan beneficiar de las nuevas tecnologías. ¡Adelante!

HOT!

NUEVO PROCESO DE FABRICACIÓN DE INTEL

La tecnología de 65 nanómetros empleada permitirá doblar el número de transistores incluidos actualmente en un chip.
Intel Corporation ha desarrollado los primeros chips SRAM (Memoria Estática de Acceso Aleatorio) utilizando tecnología de 65 nanómetros, su próxima generación de proceso de fabricación de semiconductores. Intel pretende poner en funcionamiento esta tecnología en 2005 empleando obleas de 300 mm.
Este nuevo proceso de 65 nm combina transistores de mayor rendimiento y menor consumo con la segunda generación de silicio tensionado de Intel, interconexiones de cobre de alta velocidad y un nuevo material dielectrico denominado "low-k". La fabricación de chips empleando el proceso de 65 nanómetros permitirá a Intel doblar el número de transistores incluidos actualmente en un chip. Puedes encontrar más información en el sitio http:// www.intel.com/research/silicon.

PINNACLE SYSTEMS Y FLASH MX

Pinnacle Systems, empresa líder en la fabricación y desarrollo de soluciones digitales que permite tanto a usuarios domésticos como profesionales crear, disfrutar sus vídeos y sus composiciones musicales y guardarlos en CD y DVD, ha anunciado la interoperabilidad entre sus soluciones de edición de vídeo Pinnacle Liquid & Pinnacle Edition 5.0 y el nuevo Macromedia Flash MX Professional 2004.
Con la potente funcionalidad XSend de Pinnacle, todos los usuarios de Edition y Pinnacle Liquid podrán publicar perfectamente sus proyectos y clips como objetos de vídeo Flash de forma que sus imágenes de vídeo mejorarán con la utilización de Flash MX Professional 2004, con un contenido y una interactividad específicamente orientada para Internet.
Para obtener más información, visita el sitio web de Pinnacle Systems:
www.pinnaclesys.com

SONIC, EL PERSONAJE MÁS POPULAR

Coincidiendo con el 30 aniversario del juego Pong editado por Atari, para muchos el primer video juego de la historia, la Asociación de Editores de Software de Entretenimiento Británica (ELSPA) y una prestigiosa revista online han hecho una macro encuesta entre los usuarios de este país para determinar el videojuego más popular de la historia. El elegido como videojuego más popular ha sido "Sonic the Hedgehog" por encima de clásicos como Zelda: Ocarina of Time, Pac-Man,Tomb Raider o Space Invaders, que encabezan la lista junto al popular erizo de Sega.
Yuji Naka creador de Sonic the Hedgehog comentó: "Estoy encantado y muy satisfecho de que Sonic the Hedgehog haya resultado elegido el juego más popular de los últimos 30 años, especialmente por haber tenido una competencia tan fuerte. Sonic y yo querríamos agradecérselo a los jugadores que nos han votado. Espero seguir creando juegos que gusten a todos para siempre."
Esta es la lista de los 30 mejores juegos de los 30 últimos años, según los lectores de ComputerAndVideogames.com:

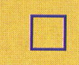
01 Sonic the Hedgehog 1991
02 The Legend of Zelda : Ocarina of Time 1998
03 Pac-Man 1983
04 Tomb Raider (Lara Croft) 1996
05 Space Invaders 1980
06 Final Fantasy VII 1997
07 Elite 1985
08 Super Mario 1985
09 Half-Life 1998
10 GTA: Vice City 2002
11 Doom 1993
12 Tetris 1987
13 Halo 2001
14 Goldeneye 1997
15 Grand Theft Auto III 2001
16 Final Fantasy VI 1999
17 Super Mario Kart 1992
18 Super Mario World 1990
19 Metal Gear Solid 1998
20 Resident Evil 1996
21 Street Fighter 1988
22 Gran Tourismo 3 2001
23 Championship Manager 1992
24 The Sims 2000
25 Quake 1996
26 Shenmue 2000
27 Lemmings 1990
28 Manic Miner 1997
29 Medal of Honor 1999
30 Asteroids 1981

Para más información, visitad el sitio web de ELSPA :http://www.elspa.com

MICROSOFT-LINDOWS: BATALLA EN EUROPA

Microsoft ha prolongado su batalla legal contra Lindows a Europe, poniendo presión sobre los fabricantes de PCs para intentar detener la distribución del software Lindows.
La disputa abre otro frente en la lucha por la marca registrada entre Lindows y Microsoft, quien arguye que el nombre de la compañía viola su marca registrada en Estados Unidos. El juicio para dirimir esta disputa está fijado para el próximo marzo de 2004.
Las acciones más recientes se relacionan con Microsoft luchando en Europa por defender lo que consideran su legítima reserva del nombre Windows. Abogados que representan al fabricante de software en Holanda, Bélgica y Luxemburgo (es decir, los países del Benelux) y en Suecia han enviado cartas a Lindows y a diversos fabricantes de ordenadores en esos países, afirmando que el uso del nombre Lindows infringe las marcas registradas de Microsoft en dichos países.
Las cartas exigen que Lindows, el fabricante radicado en San Diego, y sus revendedores dejen de ofrecer su software en estos países inmediatamente, so pena de enfrentarse a "acciones legales" sin especificar. Los abogados del Benelux, además, exigen que Lindows haga su sitio web inaccesible para los residentes en los países del Benelux.
Para saber más de esta distribución de Linux: http://www.lindows.com/

YAHOO, CONTRA EL CORREO SPAM





YAHOO!



Yahoo ha comunicado que está trabajando sobre una tecnología para combatir el spam por e-mail. Esta tecnología se basa en cambiar el modo como funciona Internet para requerir autenticación por parte del emisor de un mensaje.

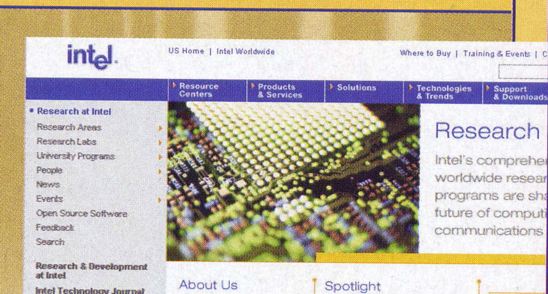
Domain Keys, el software que está desarrollando Yahoo y que espera lanzar en 2004, estará disponible libremente para los principales desarrolladores de software y sistemas de correo open source.

Bajo la nueva arquitectura de Yahoo, un sistema que envía un mensaje insertará una clave privada segura en la cabecera del mensaje. El sistema receptor podrá comprobar el sistema de nombres de dominio de Internet para localizar la clave pública registrada a nombre del dominio emisor. Si la clave pública es capaz de descifrar la clave privada insertada en el mensaje, el mensaje será válido.

OPEN LIBRARY, DE INTEL

El fabricante de chips Intel ha anunciado que ofrecerá la Open Source Machine Learning Library, una colección de programas de software que pueden ayudar a los ordenadores a aprender de distintas experiencias. Esta biblioteca se ofrecerá gratuitamente a los fabricantes interesados a través de su sitio Web.

La biblioteca está pensada para servir como un toolkit para quienes diseñan ordenadores o robots. Se basa en aprender de las acciones pasadas del usuario llevadas a cabo más frecuentemente. Encontrarás más información en http://www.intel.com/research/



MICRONET, PROVEEDOR DE CONTENIDOS



Aprovechando su tecnología de recursos online propia, la empresa española Micronet, líder en la publicación de contenidos en formato multimedia, se ha convertido en adjudicataria de contenidos educativos para la web de la Consejería de Educación de la Comunidad de Madrid, www.educa.madrid.org.

Uno de los recursos educativos más relevantes de los que podrán disfrutar los usuarios del portal de la Comunidad de Madrid será Enciclonet.com, enlace que les brindará acceso al mayor banco de información de carácter global disponible en Internet.

Asimismo, Micronet ha llegado también a un acuerdo con Pedagogía Interactiva, entidad dedicada a la prestación de servicios educativos de base tecnológica a través de su plataforma de comunicación y aprendizaje, y que recientemente ha comenzado a dar servicio las escuela del territorio español. A través de este acuerdo, www.enciclonet.com pasará a formar parte de los contenidos a los que tendrán acceso más de 40.000 alumnos en los próximos 3 años.

Enciclonet.com es una enciclopedia online, con más de 180.000 artículos. Este portal, de los pioneros en apostar por el sistema de pago por suscripción, cuenta ya con más de 150.000 usuarios registrados, 400.000 visitas mensuales y 4 millones de impresiones de páginas al mes y ha sido merecedora de diversos premios en reconocimiento a su calidad, como son el iBest 2002, el Golden Web Awards of Web Master and Designers, o el Punto de Excelencia otorgado por enelpunto.net, entre otros.

HOT!

BATERÍAS A TODA PRUEBA

Aankoop, asociación de consumidores belga, realizó un nuevo test sobre la seguridad de las baterías de los teléfonos móviles, utilizando sólo baterías originales Nokia. Los resultados de este test han demostrado sin ningún tipo de duda que las baterías originales de Nokia tienen sistema de protección anticortocircuito y cumplen todas las medidas de seguridad para los consumidores. El pasado 7 de noviembre, Test-Aankoop emitió un comunicado en el que inadvertidamente incluian baterias no originales pirateadas en el test realizado.

El pasado jueves 13 de noviembre, Nokia anunció la adopción de agresivas medidas contra los fabricantes y distribuidores de productos falsificados. Están desarrollándose los planes de actuación regional y medidas antipiratería que serán comunicados tan pronto como los programas sean oficialmente presentados.

NORTON SYSTEMWORKS 2004

Symantec ha anunciado Norton SystemWorks 2004, la nueva versión de la suite de Symantec para incrementar la productividad y resolver problemas. Norton SystemWorks 2004 incorpora un nuevo componente para la gestión de contraseñas seguras, Norton Password Manager. Esta nueva característica facilitará la labor de gestionar de forma segura largas y complejas contraseñas de aplicaciones Windows y de Internet, mientras protege dichas claves de caer en las manos equivocadas.

Norton SystemWorks 2004 también incluye la nueva versión de Norton AntiVirus, una solución antivirus de gran confianza en todo el mundo. Integrada de forma transparente con Norton SystemWorks, Norton AntiVirus sigue proporcionando una protección automática y fiable contra los virus. La nueva versión también incluye protección adicional frente a invasiones no víricas emergentes, incluidos los programas de espionaje, de adware y de grabación de pulsaciones de teclado que pueden amenazar la seguridad de un sistema, espiar los datos del usuario, o detectar el comportamiento del usuario en la red.

Puedes encontrar más información en el sitio web www.symantec.com.

El Gran Hermano se llama Palladium

Otro para Orwell: si el proyecto Palladium de Microsoft llega a buen puerto, seremos menos libres y más espiados.

QUÉ ES, CÓMO FUNCIONA Y QUÉ DESGRACIAS TRAERÁ PALLADIUM

Es inútil ocultarlo, estamos viviendo un período muy difícil. Los hechos del 11 de septiembre de 2001 han cambiado muchas cosas en el mundo que nos rodea y especialmente han sacado a la luz un aspecto del problema que antes preferíamos ignorar o, peor aún, delegar del todo a algún otro: la seguridad.
Tomando al toro por los cuernos, de modo explícito en EE.UU. y como consecuencia en Europa, los políticos se han enfrentado a una disyuntiva: **Trocar nuestra privacidad a cambio de una mayor seguridad.**
Por desgracia, bajo la onda emocional y con un empujoncito de los medios, muchas personas han respondido positivamente a esta propuesta, aunque el problema era completamente erróneo y la seguridad se podía obtener manteniendo el respeto a la privacidad y a los derechos constitucionales. La historia nos enseña, tristemente, cuán importante es para el poder político aumentar el control sobre la población, pues de ello depende su futuro. Por ello, ya hay quien ha visto en esto un negocio y ha sacado del cajón los planes ya a punto para un "ordenador seguro", que ha mostrado a todos.
El consorcio TCPA (Trusted Computing Platform Alliance) tiene su origen en el lejano octubre de 1999, cuando Compaq, HP, IBM, Intel y Microsoft pusieron las bases para **"una iniciativa centrada en mejorar la confianza y la seguridad de los ordenadores"**. Ahora esta alianza cuenta con más de 150 participantes.

El sitio de la TCPA, Trusted Computer Platform Alliance, principal promotor de Palladium: www.trustedcomputing.org.

>> Esto es Palladium

Palladium es una arquitectura de hardware y software que permite controlar todas las aplicaciones que funcionan en el PC , a partir del disco de arranque, en modo parecido al sistema de "blindaje" de la consola X-Box.
En un ordenador Palladium, ya en el momento del boot se verifica el contenido de la flash rom responsable del boot y la clave de acceso al disco, que está escrita en su interior directamente por el fabricante, para verificar que el soporte sea homologado y adaptado al estándar de seguridad. Una vez realizada la comprobación, el sistema podrá descifrar el disco y cargar "regularmente" el kernel del sistema operativo. En la fase de boot también se verifican todas las conexiones con los dispositivos, como el teclado, ya que sólo los periféricos que son reconocidos por el sistema gracias a sus claves podrán ser habilitados. El propio teclado comunica con el sistema a través de un canal cifra-

do, para evitar que pueda descifrarse fácilmente por algún programa residente. El corazón del sistema es el componente de cifrado, que según las diversas fuentes de información puede insertarse dentro de la CPU como conjunto de funciones extendidas (AMD por ejemplo) o bien como chip separado que se sobrepone entre la CPU y el resto de la placa base a caballo del south bridge (que controla el bus PCI).

Palladium gestiona todos los procesos del PC. **Antes de iniciar un proceso, éste se somete al análisis del sistema de control, el cual verifica sus credenciales (la clave) y la integridad.** ¡Pero no sólo eso! Todo archivo que se abra, se guarde o se transmita se ve sometido al mismo examen.

En consecuencia, **es posible que un mensaje de correo que habíamos guardado para su lectura posterior, se desvanezca** porque quien lo ha expedido le ha incluido una fecha de caducidad, o bien que **en el momento de reproducir un archivo Mp3 el sistema de DRM (Digital Rights Management) nos pida que demostremos que tenemos también el CD original** antes de ejecutar el clip (en este momento puede incluso cancelarlo o adquirir los derechos en modo automático/autónomo como el fabricante del reproductor haya decidido que se deba comportar).

Mario Juarez, product manager de la unidad de "content security business" en Microsoft, sostiene que "Palladium no es el DRM, sino tan sólo la plataforma ideal para construir encima un administrador de DRM", que es tanto como decir que se trata de una gran tecnología para que otro se tizne las manos.

>> Seguridad y riesgos

Todavía no se ha divulgado nada sobre las especificaciones técnicas detalladas de la arquitectura de hw/sw de Palladium, pero es cierto que Palladium se basará de todos modos en un núcleo que gestionará el cifrado de los datos, y el acceso a este trámite de las claves de longitud (y por tanto de seguridad) más bien elevada. Como en todos los sistemas de cifrado, el núcleo del problema es la seguridad real de los datos y las dudas que surgen son relativas a tres puntos clave:

- los algoritmos utilizados;
- el cifrado de todas las comunicaciones entre el PC y el administrador de recursos (y por ello no es posible saber qué datos se enviarán al administrador por Internet desde nuestro sistema);
- la eventual presencia de una puerta trasera (o Master Key) que permita a Microsoft o a un gobierno cualquiera abrir todos los archivos del sistema y por consiguiente la garantía de custodia/hurto de la propia clave.

Los algoritmos de cifrado son el producto de sofisticados y robustos sistemas matemáticos, no el resultado de una brillante intuición. Los algoritmos deben ser valorados por la comunidad porque podrían tener un talón de Aquiles que los convirtiera en presa fácil de un programador malicioso, tal vez más brillante que el titulado que ha inventado el al-

Enlaces útiles

La Faq sobre Palladium en español
http://linuca.org/body.phtml?nIdNoticia=207

Gates y China
www.cw.com.hk/Comment/c990713001.htm

InfoWorld: Microsoft serves up Palladium details
www.infoworld.com/articles/hn/xml/02/07/29/020729hnpalladium.xml

VeriSign issues false Microsoft digital certificates:
www.itworld.com/Sec/4039/IW010322hnmicro-versign/

Microsoft to reveal Palladium source code:
http://news.com.com/2100-1001-938973.html

The Big Secret
http://cryptome.org/palladium-sl.htm

10 cosas que ya no haremos

Ok, estamos jugando a adivinar, pero hemos querida probar a imaginar qué consecuencias podría tener el nuevo sistema de Microsoft sobre la actividad cotidiana de cualquiera de nosotros. He aquí una lista:

1 Ripear CD y DVD
Las conexiones entre el lector y la CPU serán cifradas, y no sería posible interceptar estos datos.

2 Descargar, ejecutar o duplicar formatos de archivo no protegidos (Mp3, Mpg, Wav, Aiff)
El sistema de Digital Right Management podría limita la utilización de todos los formatos que no utilizan un sistema de autenticación de los contenidos.

3 Usar un keylogger
Incluso los datos llegados del teclado deberán ser ci frados, por lo cual no podrán ser interceptados.

4 Usar drivers no oficiales para los dispositi vos, o dispositivos no soportados
El sistema podrá rechazar hacer funcionar un perifér co con un driver alternativo (como los de www.kxpro ject.com para la tarjeta de audio).

5 Usar software alternativo
El formato de archivo de los documentos podría se sometido a reglas restrictivas para la administració del contenido. Open Office, que utiliza formatos d archivo propietarios, podría así convertirse en ilegal.

6 Ejecutar un backup del software o de la contenidos multimedia
Una vez más, los mecanismos de control del copyrig podrían impedir operaciones perfectamente legítima como la ejecución de una copia de seguridad perso nal.

7 Usar freeware y software de bajo coste
Obtener una clave para firmar los propios programa podría tener un coste que haría imposible la realiza ción de freeware. La clave de un software no podr ser divulgada, y por ello no podrá ser publicado el c digo fuente del programa. Esto impediría la utilizació de software open source para Windows.

8 Ver películas o escuchar música en sistema no compatibles con Palladium
Las majors podrán producir CD y DVD que podrán s reproducidos sólo en sistemas Palladium, dejand fuera a todos los demás.

9 Ver algunos sitios de Internet
Dado que sus certificados no serán conformes con l de nuestro equipo, serán automáticamente oscure dos por ser potencialmente peligrosos.

10 No podremos hacer bromas a los amig
Todos los sitios, incluso los que no querríamos que supiera que hemos visitado, nos dirán al llegar: "Ha Sr. Cosme, ¿cómo está? ¿Y la familia? He visto que esposa ha comprado hace una hora una aspirina www.compramedicinas .es...

goritmo. En la práctica, no es necesario reinventar la rueda cuando están disponibles decenas de algoritmos de cifrado estables y aprobados por una amplia comunidad internacional. (AES/Rijndael, RC6, MARS, Twofish, CAST, IDEA, DES, Triple DES RC2, RC5, Blowfish, Diamond2, TEA, 3-WAY, GOST, CAST). Palladium, en este caso, debería usar algoritmos de cifrado públicos y certificados.
En cuanto a la custodia de las claves, el problema no es fácil de resolver, basta recordar un par de episodios poco edificantes sucedidos recientemente. El 29 y el 30 de enero de 2001 **VeriSign emitió por error dos certificados de Microsoft a un impostor poniendo en serio peligro a los usuarios.** Mahi De Silva, vicepresidente de VeriSign, comunicó que son los dos únicos certificados fraudulentos emitidos por error, entre 500.000 certificados emitidos. También especificó que antes de la emisión de la petición electrónica, dos personas controlan y verifican los datos manualmente. Otro ejemplo es el que ocurrió con los DVD y el DeCSS cuando todo el edificio de claves y certificados se vio comprometido por la fuga de información (un error de Xing, que divulgó la propia clave de cifrado gracias a la ingeniería inversa de su reproductor por parte de MoRE (Masters of Reverse Engineering).

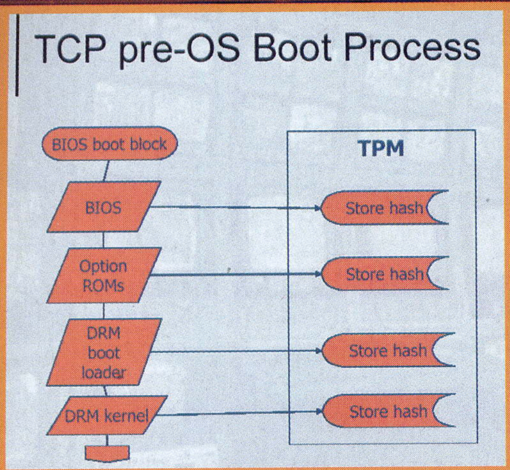
Esta es una primera versión del amigo Fritz, el procesador que gestiona el certificado en Palladium. El nombre del procesador se ha inspirado en un senador americano que ha impulsado la introducción del TCPA.

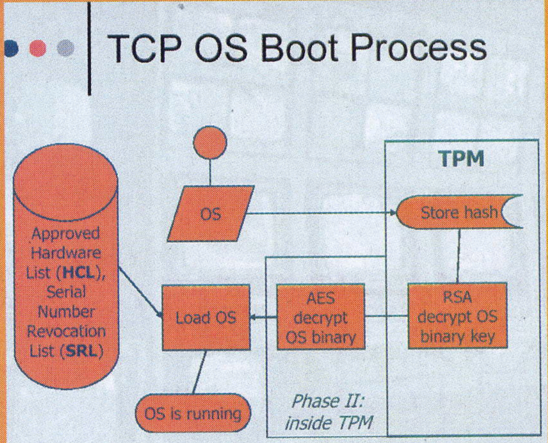
>>Open Source: la respuesta

La única solución a todas estas dudas es el Open Source. Sólo permitiendo a los usuarios verificar el código, y especialmente poderlo recompilar sucesivamente para verificar la integridad efectiva, es posible garantizar a los usuarios contra la presencia de errores grandes y pequeños, pero también ahuyentar toda duda sobre la presencia de trampas y subterfugios. Un ejemplo de esta política es la que ha seguido PGP, que, desarrollado por Philip Zimmermann con orígenes públicos, ha tenido un enorme éxito hasta la adquisición de NAI, con un bloqueo de la difusión por el temor de que la gran empresa hubiera podido insertar claves "especiales" (Master Key, en la jerga) de control bajo la presión del gobierno americano. NAI se ha visto reducida por ello a veder nuevamente PGP a una empresa privada (Pgp Corp, www.pgp .com) que volverá a proponer el producto en open source.
Durante el proceso antitrust a Microsoft, Jim Allchin, vicepresidente senior para Windows, sostuvo: "Cuanto más cosas sepan los creadores de virus sobre los mecanismos de protección del sistema operativo, más fácil será para ellos crear virus que podrán deshabilitar estos mecanismos", en apoyo de los peligros ligados intrínsecamente a la plataforma Open Source.
Por sorpresa, Juarez ha dicho, por el contrario, que el código podría publicarse, esto no significa que será Open Source, confirmando una teoría más actual que demuestra como los proyectos open source son igualmente seguros respecto a aquellos "protegidos".

Una legítima sospecha

Los analistas que tienen dudas sobre el sistema Palladium se hacen oir. Años de fracasos en el campo de la seguridad y una actitud fundamental de indiferencia frente a las observaciones de problemas de los usuarios (todo ello tapado con comunidades de prensa triunfales sobre victorias ante virus y troyanos), han llevado a una parte del público a odiar al coloso de Redmond, como si llevaran a cabo una guerra santa, a otros a dudar siempre de las palabras de Bill Gates, y a unos terceros a tener una actitud muy gélida frente a las promesas del fabricante de software.
Sin embargo, algunos datos dan argumentos para pensar que después de todo, Windows 2000 tal vez no sea peor que otros sistemas operativos: en un artículo del 24 de septiembre de 2001 y basado en las observaciones de Bugtraq, John McCormick evidenciaba que los fallos señalados eran en número absolutamente comparables a los de otros sistemas operativos, suscitando polémica y dando argumentos a Microsoft (hay que indicar que los problemas de W2K se contabilizan por separado de los de IIS, si se suman ambos Windows salta inmediatamente a la cabeza de la clasificación del dislate).





El esquema de la verificación efectuada en el boot, sacado de la presentación que Lucky Green hizo en DefCon X (la presentación se encuentra en formato Pdf y PowerPoint en www.cypherpunks.to).

Sorprendido, pero también satisfecho por las afirmaciones de Juarez, se muestra Bruce Perens, un apóstol del proyecto y creador de la propia definición de Open Source: "Creo que Microsoft está admitiendo que puede difundir el código fuente a todo el mundo, sin comprometer necesariamente la seguridad de los programas".

>>Distribución de las claves

El último problema es sin duda la distribución de las claves. Quien desarrolle un software o un sistema operativo, sin adquirir una clave no podrá distribuir su producto. Además se requiere una comisión que deberá evaluar la aplicación y ver si contiene backdoor o bien código malicioso. Todo ello hace que **el coste de una clave se eleve a valores que un fabricante aficionado de software no se podrá permitir.**

Los notebook ThinkPad de la serie T de IBM son de los primeros equipos que incorporan los circuitos para la gestión de las restricciones TCPA.

Por otra parte, ¿quién juzga si un programa es seguro? Tal vez descubramos que un sistema para ripear los CD se considera "no seguro", ante el derecho de copia de seguridad, y por ello no se le concede la clave.

¿En manos de quién queremos dejar la elección de qué software puede instalarse en nuestro PC?

>>¿Cuándo llega?

El proyecto Palladium debería ver la luz en 2004, si bien se cree que la arquitectura podría estar completamente implementada y difundida en el mercado hacia el 2006.

Mientras tanto, resulta de gran interés ver qué ocurre sobre las medidas antipiratería y DRM en la plataforma Microsoft, con la introducción del nuevo Media Player 9 pero ya presente en la versión 7, con la lectura del acuerdo de licencia que dice más o menos (traducido del inglés):

"Usted acepta que para poder proteger la integridad del contenido y del software protegido por el DRM, Microsoft puede proporcionar actualizaciones de seguridad a los componentes del sistema operativo, que podrán descargarse (e instalarse) automáticamente en su ordenador. Estas actualizaciones de seguridad podrán deshabilitar la posibilidad de copiar o mostrar el archivo con "Contenido Seguro" o el uso de otro software en el interior de su ordenador".

Sin embargo, según algunos, Palladium será verdaderamente una realidad **cuando Microsoft decida de verdad ponder freno a la piratería del software, hasta ahora de hecho tolerada**, para dar una lección a los que usan programas copiados. Bill Gates ha soñado durante años encontrar un modo de hacer pagar el software a los chinos, y Palladium podría ser la respuesta a sus plegarias: he aquí lo que dijo Gates a los estudiantes de la universidad de Washington en julio de 1999: "No obstante, en China se venden unos tres millones de ordenadores al año, pero la gente no paga por el software. Pero un día lo harán. Hasta entonces, ya que lo roban, que roben el nuestro. Así se acostumbrarán a él y luego, de algún modo, encontraremos la manera de recuperar el dinero, hacia el próximo decenio".

Para terminar, una nota histórica. Es muy divertido y sutilmente irónico que el nombre del producto, Palladium, se haya tomado de la mitología griega, dado que Paladio es el nombre del gigante matado por la diosa Atena, diosa de la guerra, de la sabiduría y de las artes liberales, pero también protectora de la ciudad de Troya, y ya sabemos que **fue expugnada por Ulises gracias a la estratagema del Caballo de Troya**. ¿Se trata de una "involuntaria" admonición? A buen entendedor, pocas palabras bastan.

Guillermo C.

UNA GUÍA PARA DAR LOS PRIMEROS PASOS EN IRC

Irc: un territorio por explorar

Para el gran público, el chat es una actividad que se puede hacer desde un sitio, desde un programa de mensajería instantánea como ICQ e incluso desde el móvil. Pero, para los expertos, el único chat verdadero es IRC.

"¿¿...Chat?? ¿Qué es esto? Ah, sí... he oído hablar de ello alguna vez en televisión o puede que haya leído algo en los periódicos..." Todavía hay personas a quienes si les preguntasen qué es un chat y, sobre todo, cómo funciona, responderían algo parecido.

El chat ya se ha convertido en un instrumento de comunicación totalmente extendido y vale la pena dedicar unas palabras a aclarar este concepto que, justamente por su gran difusión, entrará pronto en la jerga común.

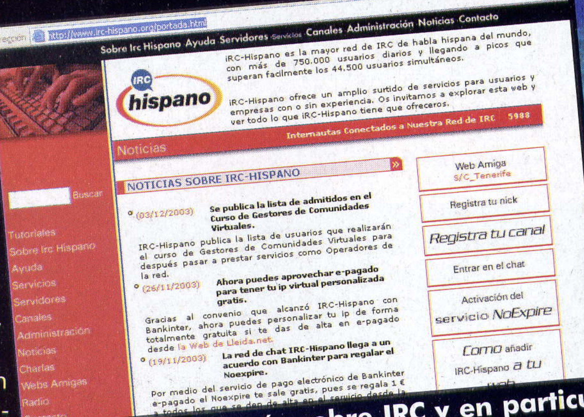
¿Pero, de qué se trata? Se trata de comunicación y, más concretamente, de comunicación activa. Navegando se puede comprar, recoger información, visitar sitios profesionales de las empresas más vanguardistas o la mísera página web del amigo "colgado" que hace sus pinitos con el HTML, pero en cualquiera de los casos, el resultado es siempre el mismo: bytes, datos, electrones, cosas inanimadas. El chat e IRC en particular como pionero, marcan la diferencia y suponen una revolución por la variedad de lo que recibimos y por proporcionar una comunicación activa y viva. Al otro lado del hilo telefónico no encontramos un servidor que pasivamente nos envía sus datos, sino a una persona de carne y hueso que nos manda sus pensamientos... ¿No os parece fascinante?

>> Los orígenes

Para situar nuestro argumento en el tiempo, diremos, de entrada, que los orígenes de IRC se remontan a hace 15 años. Fue en 1988, cuando en Finlandia, Oikarienm desarrolló su idea de chat, ampliando el clásico programa Talk, utilizado para la comunicación en red de usuario a usuario, a una de múltiples usuarios. Los primeros reconocimientos llegaron en 1991 y el año siguiente creció hasta el punto de llegar a tener 5.000 usuarios conectados al mismo tiempo, cifra considerada entonces el límite técnicamente infranqueable de la red. No muchos años más tarde, en 1999, EFnet, la más grande de las redes IRC, alcanzó los 50.000 usuarios simultáneos. Y hoy, con el aumento exponencial del uso de esta red no se puede predecir hasta donde puede llegar esta cifra.

¿Pero, qué ofrece IRC? Bueno... se podría escribir un libro de 500 páginas sólo para explicar lo que a mi me ha proporcionado, pero la respuesta más lógica a la pregunta es: "probar". Hacer nuevos amigos, conocer gente nueva, sin tener en cuenta el aspecto físico, la raza, la religión o la cultura, desarrollar una comunidad virtual de personas que viven en los lugares más dispares del mundo, gestionar proyectos comunes, encontrar consuelo, ideas, la resolución de problemas... esto y mucho más es IRC.

En la práctica, ¿cómo funciona IRC? El concepto técnico es bastante simple: todos los ordenadores se conectan a un servidor específico y cada usuario tiene un apodo o alias (en jerga nickname, o simplemente "nick"), que lo identifica de forma inequívoca y que no puede estar duplicado dentro de la misma red. Si el usuario A quiere mandar un mensaje al usuario B, este mensaje no llega directamente de A a B, concepto que estaba en la base del programa



¿Queréis saber más sobre IRC y en particular sobre los canales españoles? Visitad http://www.irc-hispano.org/portada.html

Join: Acceder. El comando Join se utiliza para entrar en un canal. "Acceder un canal" quiere decir pues "entrar en el canal". El acceso al canal permite operar en él.

LOS COMANDOS DE IRC

Entre los comandos más útiles que se pueden introducir en la línea de comandos encontramos:

/nick nick | cambia el nick al usuario conectado

/server | más el nombre del servidor al que conectar o al que se tiene que cambiar la conexión actual

/join #nombredelcanal | para conectar a un determinado canal

/whois nick | busca información sobre un nick

/msg nick mensaje | manda un mensaje a un determinado usuario

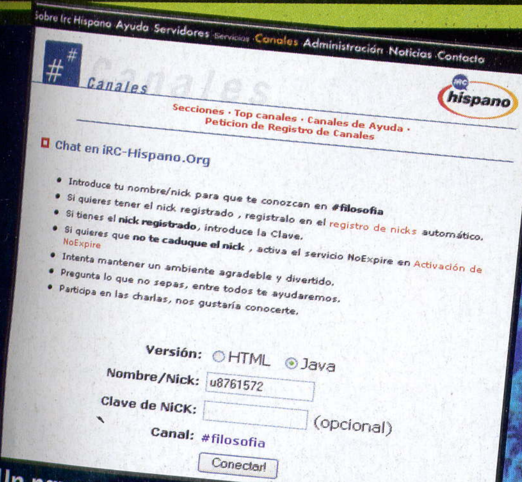
/query nick | abre una ventana privada para el diálogo con un usuario (equivalente al doble clic sobre el nick del usuario en mIRC)

/awai mensaje | Muestra el estado "ausente", especificando el motivo escrito en el mensaje

/exit | cierra mIRC







Un navegación por los sitios web dedicados al IRC os permitirá hallar canales de temas específicos. Darse de alta es muy sencillo.

Hay quien usa IRC para provocar daños, enviando virus y troyanos.

Talk, sino que pasa a través del servidor, que reconoce al remitente y al destinatario (mediante el nick) y lo manda al usuario final.
En el interior del servidor, además, se pueden crear canales con un nombre específico (#nombrecanal) donde se produce la comunicación multiusuario a la que nos referíamos antes. De este modo, cualquier cosa que se escriba en el área "pública" la pueden leer todos los usuarios conectados a aquel canal.

Query: Enviar una query (pregunta) a un usuario supone proponerle establecer una comunicación mandándole un mensaje personal, que no será visible para el resto de participantes del canal.

>> Pongámoslo en práctica

¿Pero... cómo se hace? Después de tanta teoría, veamos como se utiliza IRC en la práctica. Siendo una red formada por servidores, utilizaremos un programa cliente para el acceso, en nuestro caso, mIRC. Una vez descargado e instalado, se tendrá que configurar de la manera óptima para que funcione correctamente. En la primera pantalla que nos aparece, la de las opciones (el icono de la carpeta con el martillo), tendréis que elegir el servidor al cual queréis conectaros, especificar vuestro nombre y correo electrónico (es aconsejable utilizar el no oficial, nunca se sabe...) y elegir vuestro nickname.
En cuanto a la lista de servidores que hay en mIRC sugerimos uno de español para no tener problemas de rechazo de la conexión. Dando una ojeada a las otras opciones veréis que son todas opciones muy intuitivas, que en la mayor parte de casos no necesitan ser variadas a no ser que se quiera una personalización específica del cliente.
Del apartado DCCFolders detaca la opción DCC ignore, que sirve para ignorar automáticamente la aceptación de los archivos con extensiones especialmente peligrosas, como por ejemplo los .exe, los .pdf y los .bat. Es aconsejable activarla a no ser que tengáis mucha práctica en Internet y en ordenadores y sobre todo si no tenéis un antivirus actualizado.
Usando IRC os daréis cuenta que entre los miles de personas interesantes con las que estaréis en contacto también habrá quienes usan esta red para producir daños mandando archivos infectados con virus y troyanos. Nuestro consejo es siempre el de no aceptar nunca archivos de desconocidos, para protegeros todo lo posible de desagradables sorpresas.
Configurado adecuadamente el cliente, ya podemos introducirnos en IRC. Y una vez le damos al OK en la ventana de configuración, sólo falta conectarnos al servidor para iniciar la aventura. Hay dos maneras de hacerlo: clicar sobre el icono del rayo arriba a la izquierda o escribir /server nombredelservidor.
Se trata de un comando en línea. En mIRC hay decenas de ellos y todos empiezan con el caracter especial /. Las órdenes principales las tenéis listadas en el recuadro "Comandos de IRC".

>> ¿Y ahora?

OK, ya me he conectado. ¿Y ahora? ¡Por fin empezamos! En IRC hay miles de canales que se pueden ver con el comando /list, ¡pero, no lo hagáis! A no ser que tengáis una conexión súper rápida, el mogollón de datos que recibiréis os hará caer del servidor. De entrada, es mejor empezar



Take: El término inglés significa en español tomar. Un canal se dice que está tomado cuando ha sido robado a sus legítimos propietarios.

Clientes para todos

Si en Windows la mayoría de los usuarios utiliza mIRC (www.mirc.com) como cliente de chat, en Mac y Linux no hay un predominio absoluto. En cuanto a Mac, probablemente el client más difundido es Ircle (www.ircle.com), para el cual existen numerosos sets de script ya a punto (sólo hace falta buscar Ircle en versiontracker.com para encontrar un montón). Un programa más reciente pero que se está extendiendo es Snak (www.snak.com), menos completo pero quizás más inmediato e intuitivo. Ambos son compatibles con los sistemas tradicionales y con el nuevo MacOS X.
Quien prefiere un cliente lanzado bajo licencia GPL puede dirigirse a ShadowIrc (www.shadowirc.com), aunque este no es compatible nuevo Mac OS X.
En cuanto a Linux, el cliente más famoso de linea de comando es probablemente BitchX (www.bitchx.org), totalmente escriptable y programable, aunque poco adecuado para noveles o débiles de corazón. Un cliente más fácil de utilizar podria ser XChat (www.xchat.org), que tiene una interfaz gráfica XFree86.





con el canal de vuestra ciudad: probad con #madrid, #barcelona, #valencia, #bilbao, todos accesibles con el comando /join #nombrecanal... De vez en cuando alguno de esos no funciona, podeis probar variantes como #madrid1, #madrid2... ¡Quizás tengáis suerte!

El mejor método para conocer canales sigue siendo el persona a persona, buscad a gente con vuestros intereses, preguntadles si conocen canales temáticos o sitios web en los que se hable de lo que os gusta y ya veréis que pronto vuestra lista se llenará de canales por visitar... :D

Bien, ahora que ya estáis dentro, por fin empezáis a hacer querys a los presentes (intentar establecer un contacto directo con otro nick) y veis cómo va vuestro primer encuentro. Si nadie os responde podría significar que hubieseis contactado un grupo de maleducados, pero sin duda esta no es la filosofía de IRC y lo más probable es que hayáis contactado con nicks equivocados.

>> Operadores y bots

Sobre la lista de cada chat hay varios usuarios con una @ delante de su nick. Algunos de ellos son humanos y son los operadores que os decía antes, otros son bot (robots). Los operadores son superusuarios, cuya función es el control del canal con capacidad de expulsar (/kick) y vetar (/ban) a los usuarios indeseados.

Con el comando /kick, un operador puede echar temporalmente a un usuario de un canal, mientras con /ban puede impedirle volver a entrar (es decir que puede vetarlo en el canal).



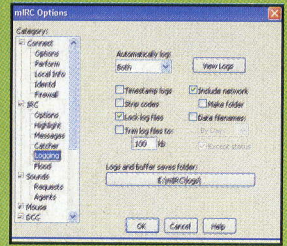
DCC: Direct Client Connection. Protocolo para el intercambio de datos entre dos clientes.

BOT es una contracción de la palabra robot. Se trata de programas que llevan a cabo acciones en un canal IRC. Se montan en clientes perennemente conectados a IRC y tienen funciones de súper usuario, controlando que en el chat no haya problemas y procurando que la actividad se desarrolle siempre de la mejor de las maneras. Los BOT son inanimados, son gestionados por administradores del canal que los programan. No os ofendáis si no os responden... ¡¡Simplemente, no pueden hacerlo!! Intentadlo con algún usuario sin la @, con un nick que veis chatear en público. ¡Sed corteses y nadie os negará nunca un caluroso "bienvenido a nuestra comunidad"!.

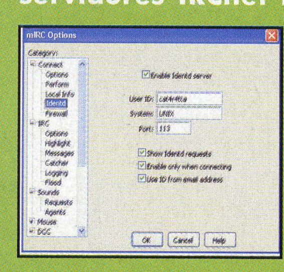
Operador: usuario con privilegios especiales en el interior del canal.

Espero que este breve paseo por IRC os haya servido para haceros una somera idea de lo que es esta red, de qué se puede hacer utilizándola y cómo empezar a hacerlo. En próximos números entraremos más a fondo en el tema. Analizaremos de una manera mucho más técnica la comunicación, cómo crear y administrar un canal, quién son y qué hacen los operadores, los comandos del servidor disponibles, qué es y cómo se configura una IPv6, la dshell, la configuración de los BOT, los servidores IRC y los problemas de seguridad del IRCwar.

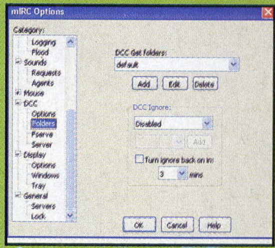
CAT4R4TTA



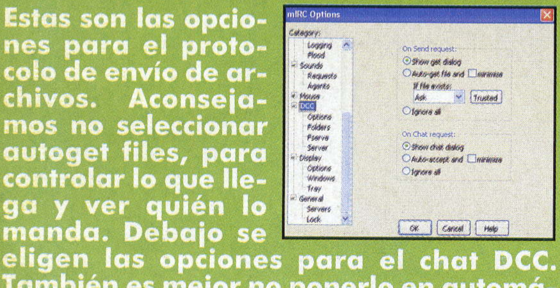
En mIRC es posible registrar las actividades llevadas a cabo. En el primer menú, en un desplegable se elige entre las querys, el canal público o ambos, en las opciones se decide el estilo y tamaño de los archivos y en la última línea se selecciona la ruta preferida.



Algunos servidores requieren un cliente para permitir la conexión. En general los servidores IRCnet no la requieren, decidid vosotros si queréis usarla o no.



En el menú desplegable DCC ignore podemos elegir las extensiones de los archivos que no deseamos (por ejemplo *.exe, *.bat, *.pif). Si sois usuarios novatos os conviene activarlo para evitar sorpresas desagradables.



Estas son las opciones para el protocolo de envío de archivos. Aconsejamos no seleccionar autoget files, para controlar lo que llega y ver quién lo manda. Debajo se eligen las opciones para el chat DCC. También es mejor no ponerlo en automático para evitar querys no solicitadas, a veces utilizadas también con fines no precisamente amistosos (...dccfucker...).

Ventana principal de conexión: podéis elegir la red (IRCnet, EFnet, iRC-Hispano...) y el servidor relativo. Es mejor seleccionar servidores españoles, porque a menudo los extranjeros no permiten conexiones de IP de "fuera del país". En la segunda mitad podéis poner vuestro nombre y correo electrónico (mejor si no es el oficial) y decidir vuestro nick.

No hay que explicar nada difícil. Dad una ojeada y elegid las que os parezcan más útiles.



...Y te infecto un archivo

¿Estáis seguros de verdad que detrás de aquel inocuo salvapantallas de simpáticas y desnudas señoritas no se oculta un peligroso caballo de Troya?

Muchos saben que es posible infectarse con un virus de origen desconocido a través del correo electrónico o colocando un CD de procedencia desconocida en el ordenador, **pero infravaloran la posibilidad de ser infectados con otros métodos, que son tan simples como eficaces.**

Estos otros métodos de difusión de virus los utilizan piratas que lo que buscan es apoderarse del ordenador de la víctima, instalando, por ejemplo, un caballo de Troya como Back Orifice, NetBus o sub7.

A modo de ejemplo: el software NetBus se divide en dos partes, Netbus.exe y Patch.exe. Este último es el que infecta el ordenador de la víctima y naturalmente se tiene que ejecutar en su ordenador. ¿Pero, cómo se infecta a la víctima con el archivo Patch.exe?

INSTRUMENTOS ANTI TROYANOS

A menudo un antivirus actualizado no es suficiente para identificar con seguridad un troyano. Para estar tranquilos de verdad conviene usar uno de estos programas:

Anti-Trojan
www.anti-trojan.net

SwatIt Trojan Scanner
www.lockdowncorp.com

Trojan Remover
www.simplysup.com

Tiny Trojan Trap
www.tinysoftware.com

Trojan Guarder
www.your-soft.com

>> Pegar dos archivos

Una técnica utilizada por los piratas es la de **pegar el archivo virus.exe a un software limpio**, utilizando programas con esta función y con pocos clics de ratón.

Uno de los muchos programas que se utilizan puede ser EXE JOINER o bien JOINER BY BLADE, que utiliza el mismo principio, pero que también funciona con otro tipo de archivos (jpg, bmp, etc.). Crea un archivo que ejecuta uno detrás del otro los dos precedentes (en el caso de un jpg y un exe, muestra el jpg y ejecuta el exe).

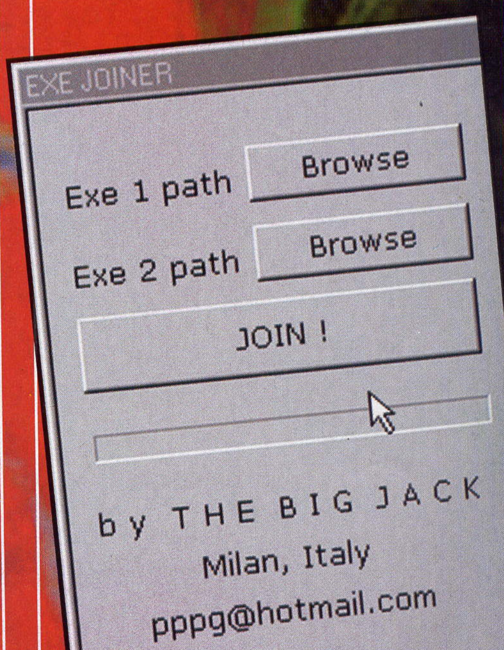
El programa EXE JOINER es de una simplicidad increíble de modo que lo puede utilizar cualquier colgado que sepa encender el ordenador y ejecutar un programa. Basta con clicar sobre "Browse" Exe 1 path y buscar el archivo .exe limpio (por ejemplo un programa para comprimir archivos como WinZip.exe) y seleccionar "Browse" Exe 2 path para buscar el archivo infectado que se tiene que pegar al programa limpio (como Patch .exe en NetBus). En este momento seleccionando JOIN el programa une los dos archivos en uno .exe. Basta distribuir el WinZip infectado para pillar víctimas. Otra posibilidad es actuar desde un pequeño sitio construido con este fin. Cuando la víctima abra file.exe junto con el software limpio también instalará sin saberlo el virus.

>> ¡En guardia!

No es suficiente, pues, estar atentos a los archivos adjuntos al correo electrónico, sino también a los programas aparentemente "limpios" que descargamos de Internet. Es por ello que es importante **descargar software únicamente de sitios fiables o analizarlo a conciencia con un buen antivirus** antes de llevar a cabo su instalación.

Si estáis buscando material que se encuentra sólo en sitios que no se pueden considerar fiables, como mínimo, efectuad un buen análisis con un antivirus actualizado, y si es posible, probadlo en un ordenador que no contenga datos importantes para vuestro trabajo o estudio. Después de la instalación, **utilizad un software para detectar troyanos** y controlad siempre que en vuestro ordenador no haya programas server que no conocéis.

Michele A.



Basta dar una ojeada a un programa como ExeJoiner para entender lo fácil que es para un lamer colocar un programa maligno dentro de otro de aparentemente inocente.

DE JULIO CESAR A IBM

Hace siglos que los matemáticos libran una batalla entre ellos: unos intentan inventar códigos de cifrado inviolables; y otros hacen de todo para envanecer los esfuerzos de los primeros.

Para comprender cómo funcionan los sistemas de criptografía modernos, debemos partir de lejos. Para ser precisos, nos remontamos a los mensajes que César enviaba a sus tropas. Para evitar intercepciones, César escribía los mensajes transcribiendo las letras. En esencia, un mensaje con clave 3 usaba un alfabeto según el cual A=D, B=E, C=F, etcétera. Naturalmente, un cifrado de este tipo funcionaba sólo en la época romana, porque **hoy cualquiera puede descifrar un mensaje de este tipo usando solamente papel y lápiz**. . Las claves de cifrado, de hecho, son sólo 26, tantas como las letras del alfabeto. Naturalmente, hay que descartar la primera porque corresponde al texto en claro (A=A, B=B, etc.). Algunas mejoras se obtuvieron haciendo corresponder letras casuales a las letras del alfabeto, pero el sistema resultaba complicado, el cambio de los códigos era liado y sobre todo la operación resultaba inútil, ya que con un análisis estadístico de los caracteres cifrados era posible llegar a los caracteres "en claro" confrontando la frecuencia con los que se usan normalmente.

>> Complicar las cosas

Una evolución del sistema usado por César se llamaba "código de Vigenere" y se basaba en una tabla cuadrada que tenía en la primera línea el alfabeto normal y en las siguientes todas las combinaciones usadas en el sistema de cifrado de César. Ante todo se tenía que elegir una clave. Después se escribía a modo de repetición la clave bajo el mensaje a cifrar. Para acabar se cifraba cada letra del mensaje utilizando el código correspondiente a la línea de la letra de la clave. Por ejemplo, para cifrar el mensaje "Estoy comiendo una manzana" usando la clave "camino" se escribía bajo el mensaje "caminocaminocaminoc". Después se cifraban individualmente las letras según las claves dadas por las letras de la clave. Por ejemplo, con clave "c" la letra correspondiente a la "s" del texto en claro era la "u". al final se obtiene una cosa tipo "guvqaeqokgpfqxpcocpbcpc" que descodificado con la clave "camino" y el mismo sistema nos da el mensaje original. El verdadero problema de este sistema sale a la luz a mitad del 800 porque se notó que en mensa-

A	C	A	S	E
B	D	B	T	F
C	E	C	U	G
D	F	D	V	H
E	G	E	W	I
F	H	F	X	J
G	I	G	Y	K
H	J	H	Z	L
I	K	I	1	M
J	L	J	2	N
K	M	K	3	O
L	N	L	4	P
M	O	M	5	Q
N	P	N	6	R
O	Q	O	7	S
P	R	P	8	T
Q	S	Q	9	U
R	T	R	0	V
S	U	S	A	W
T	V	T	B	X
U	W	U	C	Y
V	X	V	D	Z
W	Y	W	E	1
X	Z	X	F	2
Y	1	Y	G	3
Z	2	Z	H	4
1	3	1	I	5
2	4	2	J	6
3	5	3	K	7
4	6	4	L	8
5	7	5	M	9
6	8	6	N	0
7	9	7	O	A
8	0	8	P	B
9	A	9	Q	C
0	B	0	R	D

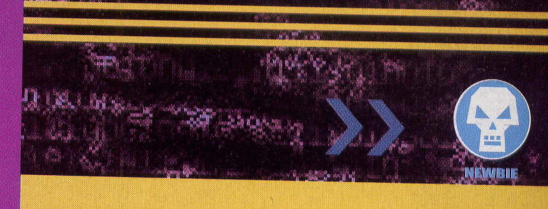
La codificación y descodificación con el sistema de Vigenere es banal. Se escoge una clave (en este caso, "case") y se escribe repetidamete bajo el texto a descodificar. Después se buscan las letras que componen el texto a codificar en la columna correspondiente a la "A" y se transcribe la letra en el cruce entre la letra del texto "en claro" y la de la clave. Hoy día se descodifica fácilmente incluso sin clave recurriendo a sistemas "de fuerza bruta" o a análisis de frecuencia de los códigos e hipótesis sobre la longitud de la clave.

ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890

Para interpretar el código usado por Julio César, basta una simple regla con una barra corredera sobre la que se escriben las letras del alfabeto. Haciendo correr la parte inferior se cambia la "clave" necesaria para la descodificación. Esta operación solía hacerse manualmente o se recorría a dos ruedas fijadas en el mismo perno, de las que la superior era más pequeña. Haciendo rodar la más pequeña se creaban nuevas correspondencias con la más grande. Para comprenderlo sin poseer la "clave", bastaba con algún intento con papel y lápiz.

EL ALGORITMO DE IDEA

El sistema de funcionamiento de IDEA es muy similar al que usa DES, con la diferencia de que el texto a cifrar está dividido en bloques de 64 bits, cada cual dividido en otros subbloques de 16 bits. La función de "scrambling" usada por DES es sustituida por una función que se ocupa de cumplir otras operaciones de XOR, sumas y multiplicaciones en base 16. Cada subbloque está sometido a 8 pasajes durante los que el segundo y el tercero cambian de lugar.
Resulta interesante notar cómo por el uso de este sistema se generan 52 claves distintas. La clave originaria de 128 bits se divide en bloques de 16 bits que constituyen las primeras 8 claves. Después, los bits que componen la clave original se mueven 25 bits a la izquierda, generando una nueva clave que viene dividida en 8 claves secundarias. El procedimiento sigue con desplazamientos y divisiones hasta generar todas las claves necesarias.
El sistema de funcionamiento de IDEA, como el del DES, es muy conocido por la comunidad científica y se encuentra fácilmente en Internet usando cualquier motor de búsqueda.



jes largos algunos caracteres tendían a repetirse en la misma secuencia. Para traducir un mensaje de este tipo basta analizar un texto muy largo o más textos con la misma clave, encontrar el máximo común divisor de las distancias entre las secuencias idénticas y aparece la longitud de la clave. **Una vez identificada la longitud de la clave podremos proceder a intentar el descifrado** ya que todo se reduce a una serie de cifrados de César.
Otro sistema de cifrado consistía en la transposición del mensaje, en una remezcla del mensaje según una cierta clave. Se escogía como clave del mensaje una palabra que no contuviera letras dobles. Después se escribía el mensaje bajo la palabra, volviendo a empezar cada vez que se llegaba al final de la palabra.
De esta manera se formaban tantas columnas de letras como tenía la palabra clave. Después se transcribía el mensaje ordenando las columnas transcritas en base a la posición de las letras de la palabra clave. Por ejemplo, supongamos que usamos la palabra clave "marco" y codificamos el mensaje "Hoy he ido a hacer una excursión al lago". Bajo la "m" de la palabra clave encontramos las letras "hianung". Reordenando alfabéticamente las columnas en base a las letras de la palabra clave tendremos una remezcla del mensaje con el orden de columnas "a" "c" "m" "o" "r". El mensaje resultante será "odcaraoharxilhianungehaucoayoeesl". Aunque el descifrado puede parecer muy complicado **en realidad es posible romper el código emitiendo hipótesis sobre la longitud de la clave en varias tentativas**. La famosa máquina ENIGMA usada por las tropas alemanas durante la segunda guerra mundial no era más que un sistema mecánico de cifrado que usaba el método aquí visto aplicándolo más veces en repetición y codificando el texto ya codificado.
El DES es el primer sistema de cifrado que se ha aplicado como estándar. En 1977, después de su desarrollo por parte de IBM y sucesivas modificaciones por parte de la agencia de seguridad nacional de los EE.UU. se introdujo para la protección de datos no clasificados como secretos de estado o militares. Se trata de un sistema de codificación que usa una clave de codificación de 64 bits dividida en bloques de 8 bits cada uno. El último bit de cada bloque se usa para el control de los precedentes, por lo que la clave es propiamente de 56 bits.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1
3	4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2
4	5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3
5	6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4
6	7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5
7	8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6
8	9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7
9	0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9

La tabla usada para codificar el código de Vigenere recogía todas las combinaciones posibles del código de César y las usaba junto a una clave para obtener el código cifrado. Estuvo en uso hasta el 800 porque el código obtenido era difícilmente analizable. Ya no se consideró fiable cuando se notó que en los mensajes largos algunas secuencias de letras codificadas se repetían y permitían un análisis manual.

>> DES e IDEA

La escasa longitud de la clave ha sido la fuente de numerosas polémicas referentes a la elección "guiada" por la NSA hacia la adopción del DES. En 1998 la EFF (Electronic Frontier Foundation) anunció el nacimiento del primer sistema de hardware para la descodificación de mensajes que usan DES. En el año 2000 el DES pasa a la historia porque la información para construir un DES-Cracker está ya al alcance de todos.
El sucesor de DES es IDEA, un sistema de codificación parecido al DES que usa claves de 128 bits. Esto permite obtener una mayor seguridad debido a que las posibles combinaciones para la descodificación son 2^128, suficientes para desanimar a cualquier simple analista e incluso a la mayor parte de los gobiernos.

Khamul

El algoritmo del DES

El texto por cifrar se divide en bloques de 64 bits. Cada bloque cambia de posición con otro y se divide en dos bloques de 32 cada uno. Después se aplica una función por 16 veces que transpone y sustituye cada mitad del bloque usando una clave obtenida matemáticamente desde la clave original. Durante cada paso las dos mitades del bloque se cambian de lugar.
El algoritmo es recursivo y los cambios operados en los datos son notables.

El bloque total es igual al medio bloque izquierdo seguido del medio bloque derecho en un cierto paso indicado con "n".
T(n)=L(n)R(n)

El medio bloque de la izquierda es igual al medio bloque de la derecha del paso precedente (n-1).
L(n)=R(n-1)

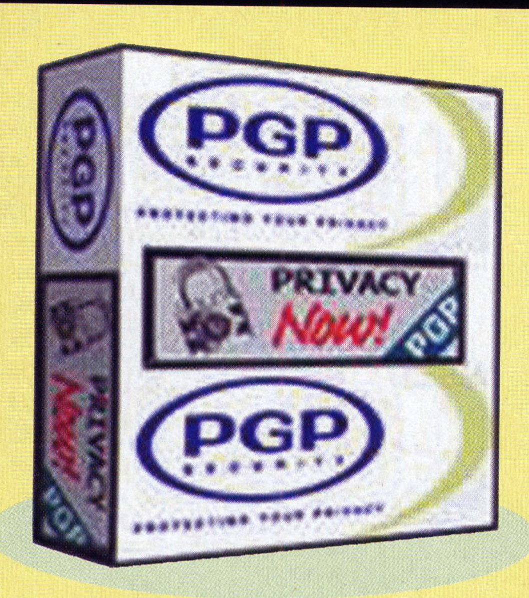
El medio bloque de la derecha es igual al medio bloque de la izquierda del paso precedente en el que se ha hecho una operación de OR exclusivo (XOR) confrontándolo con el resultado de una función que involucra a la clave. Esta clave se construye matemáticamente en cada paso obteniéndola a partir de la clave original. Por tanto, cambia a continuación según el valor de n.
R(n)=L(n-1) XOR función[R(n-1),CLAVE(n)]

La función aquí vista es bastante complicada, pero no inaccesible.
Primero, el bloque R(n-1) de 32 bits se expande para que ocupe 48 bits. En este bloque expandido se hace una operación de XOR (OR exclusivo) respecto a la clave usada para este paso. El resultado de la operación se fragmenta en 8 bloques de 6 bits cada uno. Cada bloque es procesado por una función que controla algunas matrices fijas (llamadas S-box) retirando de ellas hebras de 4 bits identificadas en base a los 6 bits de entrada. Cada bloque de 4 bits se reengancha a los otros bloques cambiándolos de lugar entre ellos. El resultado de salida es un nuevo bloque de 32 bits pero codificado a través de la operación de XOR con la clave y la sustitución con los valores de las S-Box.

CÓMO USAR E INSTALAR PGP, EL PROGRAMA DE CRIPTOGRAFÍA MÁS FAMOSO

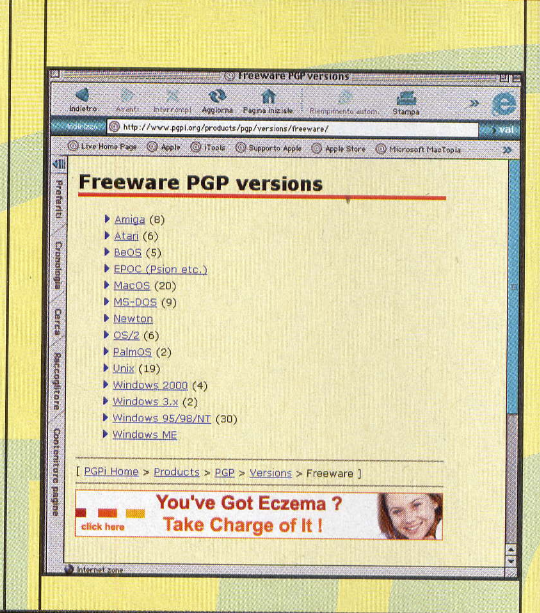
PON LOS DATOS LEJOS DE

Olvida las docenas de "softwarcitos" que prometen cifrar tus documentos: el único



"PGP permite a la gente común y corriente tener la propia privacidad a su alcance. Hay una necesidad social creciente de esto. Por eso lo he creado." Éstas son palabras de Philip Zimmermann, el padre de PGP. Qué es PGP? PGP pertenece a Pretty Good Privacy y es un software desarrollado en 1991 por Philip Zimmermann, que permite criptar mediante un sistema de claves cualquier tipo de dato, para garantizar la privacidad, por ejemplo, en el intercambio de información vía e-mail o cualquier otro sistema. Hoy día PGP existe en muchas variantes y su uso está muy difundido. Criptar los datos que intercambiamos cuando enviamos y recibimos mensajes de correo electrónico, por poner el ejemplo más banal (pero también cuando chateamos por ICQ o enviamos archivos a alguien), tendría que ser, sobre todo para quien se interesa por todas la problemáticas relativas a la seguridad, una práctica común. El derecho y la necesidad de tener una buena privacidad van más allá del contenido de los datos que decidimos criptar; es decir, no es necesario tener "alguna cosa para esconder" para usar un software como PGP; como sabiamente afirma Zimmermann, es hija del buen sentido común la necesidad de tener la propia privacidad al alcance. Dejando aparte por un momento estas reflexiones sobre la privacidad, vamos a ver

GPG Si bien las fuentes están libremente disponibles, PGP es una propiedad intelectual. Existe una versión completamente libre, llamada GPG, publicada bajo licencia GPL (www.gnupg.org).









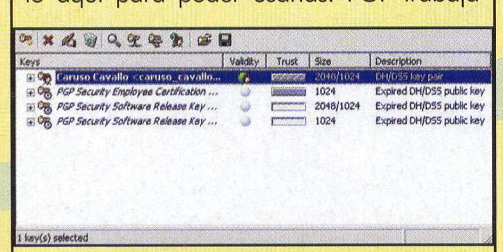
MIRADAS INDISCRETAS

programa que merece nuestra consideración es sin duda Pretty Good Privacy.

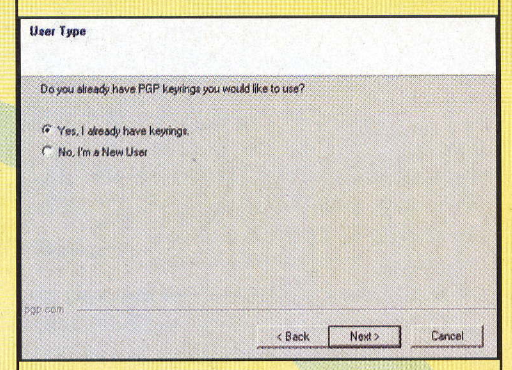
cómo se pone en práctica. Nos ocuparemos de PGP en Windows, de su instalación y de su uso en el trabajo cotidiano. Iniciamos con la descarga de PGP para Windows, por ejemplo de aquí:
http://www.pgpi.org/products/pgp/versions/freeware/
En este sitio (que es el del proyecto internacional PGP) también podremos encontrar numerosas implementaciones de PGP, además de versiones diversas del software para numerosos usos y numerosos sistemas operativos. El paquete para Windows 2000 pesa casi siete megas. Una vez ultimada la descarga nos encontraremos delante del usual archivo .zip, que contiene el programa. Al iniciar la instalación, la primera cosa que se nos pedirá es si somos nuevos usuarios o si poseemos ya un "manojo de llaves" para importar.

>> Claves digitales

Las claves PGP no son más que una serie de datos usados para criptar y desencriptar la información. Si por ejemplo tuviéramos ya nuestras claves para descriptar nuestros viejos documentos, deberemos especificarlo aquí para poder usarlas. PGP trabaja

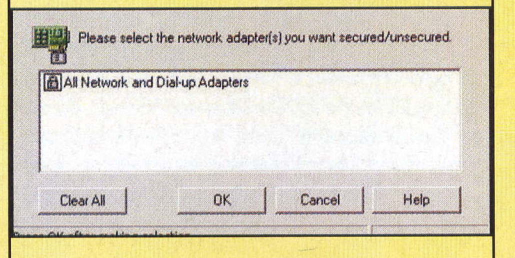


con un par de claves, una pública, libremente distribuible para permitir a otros que nos envíen material cifrado, y otra privada, que debe custodiarse celosamente y no revelar nunca a nadie.
Supongamos que somos nuevos usuarios y sigamos el asistente de instalación nos

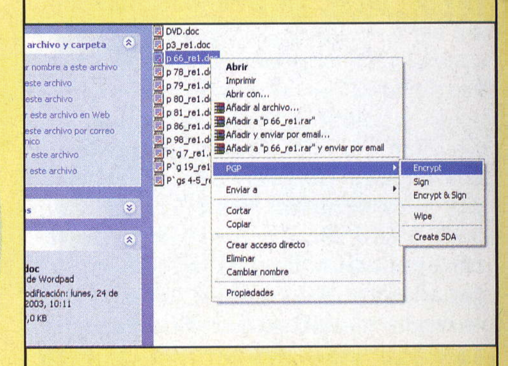


pedirá que especifiquemos qué componentes y qué plugins deseamos instalar. Dejemos seleccionadas las opciones preconfiguradas. Los distintos plugins resultan muy útiles porque integran PGP en muchas

aplicaciones comunes como Outlook, ICQ o Eudora, de modo que hacen muy simple, por ejemplo, el envío de e-mails criptados. En la práctica, encontrarás en la barra de botones de tu cliente de correo electrónico los relativos a PGP, y esto te ahorrará tener que hacerlo todo manualmente. En el paso siguiente nos pedirá qué dispositivos de



comunicación deben tomarse en consideración (tarjetas de red y/o módem). Llegados a este punto, el wizard iniciará la instalación propiamente del software. Entonces será el momento de crear nuestras claves (las que, como ya hemos dicho, nos consentirán efectivamente criptar los datos). Nos pedirá una identidad (nombre y e-mail) y una pass-phrase, es decir una frase que el software utilizará para generar las claves. La frase debe ser suficientemen-



te compleja. Al terminar, después del acostumbrado reinicio del ordenador, podremos ver que entre los iconos tray de nuestra barra ha aparecido el relacionado con PGP.
Clicando este icono con el botón secundario podremos seleccionar las herramientas de PGP, configurar las opciones o trabajar con nuestras claves, añadir usuarios, etc.
Llegados a este punto PGP se ha instalado correctamente en nuestro ordenador. Dando una vuelta por el disco duro y clicando con el botón secundario del ratón sobre un archivo cualquiera podremos notar la integración de PGP con el sistema operativo.

>> ¡Conviene usarlo!

Una vez acostumbrados, usar PGP será bastante simple, y decididamente aconsejable. Es la mejor herramienta para proteger nuestros documentos de ojos indiscretos que por desgracia abarrotan la red.





Navegar anónimo con el mínimo esfuerzo

¿Estás harto de retocar cada vez la configuración de los proxys para poder asegurarte un poco de sano anonimato en la red? ¡He aquí el programa que necesitas!

Se sabe que cada vez que se visita un sitio, éste podrá obtener toda una serie de informaciones, a partir de la dirección IP (de la que se puede remontar a grandes líneas a la posición geográfica) hasta la dirección de procedencia, el sistema operativo y el navegador.
Uno de los métodos más usados para esconder el propio rastro es el uso de un servidor proxy, un ordenador intermedio entre nosotros y el destinatario de la conexión. En lugar de ver nuestras "huellas digitales" (en el sentido más moderno de la palabra) el sitio visitado verá la dirección y la información del proxy.
Los proxys pueden ser utilizados por una interfaz Web (como la de anonymizer.com) **o modificando la configuración de red** (o la del navegador). El problema en el último caso es que a menudo los servidores proxy nacen y mueren en pocos días, o en ciertos momentos están tan abarrotados que son casi inutilizables, y es necesario a menudo buscar uno que funcione y modificar la configuración.
En resumen, después de un rato la cosa podría resultar molesta. Si no tienes exigencias dignas de un 007, te puede ser muy útil la utilidad MultiProxy, que mantiene una lista de proxys, que se controlan para verificar su fiabilidad y velocidad cada vez que se inicia el programa. Se ocupará de ordenarlos por velocidad, eliminar los que no estén activos (o que no sean seguros) y seleccionará el mejor y más adecuado en cada momento.

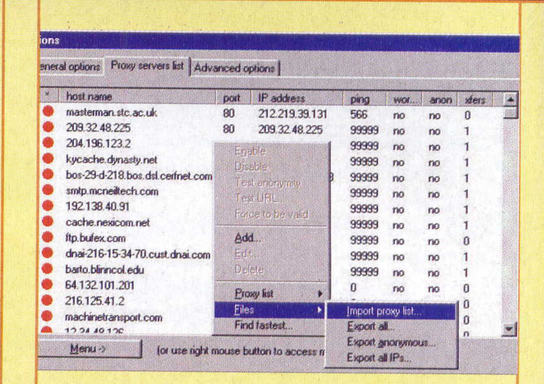
1 Como siempre, lo primero es descargar el programa de la dirección www.multiproxy.org, e instalarlo en el ordenador con un doble clic sobre el archivo .exe que se obtiene después de descompactar el archivo .zip descargado.

2 Como segundo paso, hará falta procurarse una lista de proxys actualizada. La que se encuentra en el sitio tiene fecha de mayo; para algo más reciente puedes probar en **www.atomintersoft.com/products/alive-proxy/proxy-list/**, procurando escoger solamente proxys anónimos.

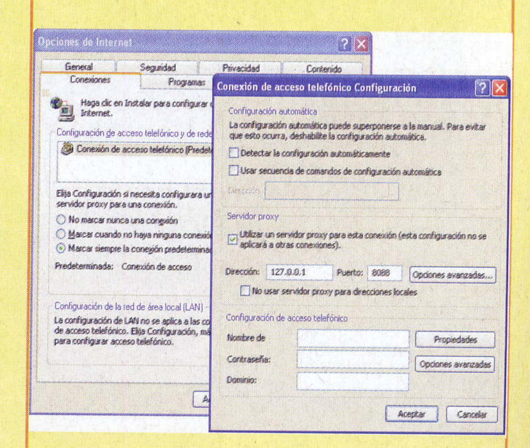
3 Abre el Bloc de Notas y crea un archivo de texto que contenga las direcciones de los proxys, uno por línea. Después de abrir MultiProxy con un doble clic sobre su icono, haz clic en Options, y luego sobre la lengüeta Proxy servers list. Haz clic con el botón secundario y selecciona el comando Import Proxy List del menú Files, seleccionando el archivo que has creado hace un momento.

```
dnai-216-15-34-70.cust.dnai.com:80
barto.blinncol.edu:8080
64.132.101.201:8080
216.125.41.2:80
machinetransport.com:80
12.34.48.126:80
12.34.48.129:8080
206.8.102.102:80
216.102.13.21:80
64.132.101.212:8080
216.101.117.161:8000
63.238.139.7:80
64-93-37-226.client.dsl.net:80
216.167.107.64:8080
cmas-tj.cablemas.com:8080
207.225.81.150:80
12.34.48.129:80
webmail.mail-ahoy.com:8000
```

4 Ahora cierra la ventana Options y pulsa el botón Check all proxies: verás iniciar un contador a mano izquierda, que muestra el estado de avance de la verificación de las condiciones de los distintos servidores. Espera a que llegue al final. En la ventana Proxy Servers list ahora debería aparecer la lista de proxys con una bolita verde en los que están activos y una roja en los inactivos.



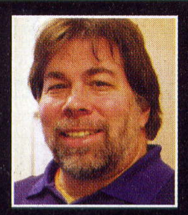
5 Ahora abre el navegador y, en la configuración del proxy http, inserta la dirección 127.0.0.1, y el puerto 8088. Si utilizas Internet Explorer 6, selecciona Opciones de Internet del menú Herramientas y haz clic sobre la lengüeta Conexiones, o selecciona la conexión de Acceso Remoto deseada, pulsa el botón Configuración, haz clic sobre la casilla Utilizar un server proxy para esta conexión e inserta la dirección como se ve más abajo.



Llegados a este punto, cada vez que pidas una dirección de Internet con tu navegador, éste no contactará con ella directamente, sino que hará una demanda a MultiProxy, que te conectará al proxy más veloz de su lista y te permitirá una navegación por fin reservada.

DE LAS CAJITAS PIRATA A UNA EMPRESA MULTIMILLONARIA

Steve Wozniak, el mago de Woz



Ida y vuelta a las altas esferas de la industria hi-tech, empezando como constructor de tarjetas pirata para acabar como profe en la escuela media.

Steve "the Woz" Wozniak es un personaje muy singular en la historia de ordenador. Es uno de los fundadores de Apple, junto a Steve Jobs, y se puede decir que ha inventado el ordenador personal de masas (con el Apple I y sobre todo con su sucesor, el Apple II). No obstante, lo ha abandonado todo, fama y dinero incluidos.

>> Exordios piratescos

Si el final de la carrera de Wozniak en la industria hi-tech es singular, los inicios no lo son menos. El primer dinero lo ganó vendiendo aparatitos electrónicos que construía él mismo: los 'Blue Box'. **Los Blue Box son cajitas con un generador de frecuencias de audio que, al lado de un aparato de teléfono, permitían telefonear gratis** a cualquier parte del mundo. Se puede imaginar hasta qué punto estos aparatos llegaban a ser útiles a los estudiantes de la universidad de Berkeley, que estudiaban lejos de familiares, amigos y parejas. Ya entonces empezaba a delinearse el orden que luego habría tenido la sociedad de la manzana coloreada: **Wozniak creaba circuitos cada vez más refinados y Steve Jobs (actual administrador delegado de Apple) se ocupaba de comercializarlos** en los dormitorios del campus y de expandir el mercado.

En aquellos tiempos, Woz hacía trabajos para Hewlett Packard y había empezado a proyectar el Apple I, casi para divertirse. Para Woz, **el Apple I era la chispa que habría podido desencadenar la revolución del ordenador personal**; las posibilidades de ganancia no le interesaban demasiado. Woz sometió el proyecto a su jefe en HP, quien sostenía que un ordenador de 800 dólares que pudiera ser conectado a la televisión y programado en Basic era una cosa demasiado arriesgada para una sociedad que, como HP, había fundado su fortuna en productos profesionales y fiables.

>> Salto de calidad

Intuyendo que se trataba de un producto revolucionario, Steve Jobs empujó Wozniak a reclamar a HP una declaración liberatoria que le reconociera la propiedad intelectual del Apple I (según HP, todo lo que venía producido por Wozniak pertenecía a la compañía). **Wozniak, Jobs y algunos amigos empezaron a producir el Apple I en el garaje de Jobs y a venderlo por correspondencia.** El enorme éxito de la iniciativa facilitó a Jobs el trabajo de encontrar capital para transformar el grupo de hackers en una empresa. Empresa que muy pronto resultó demasiado grande y demasiado compleja para un espíritu como el de Woz, más interesado en los aspectos científicos, tecnológicos y sociales de sus propios proyectos que en las cuestiones organizativas y financieras.

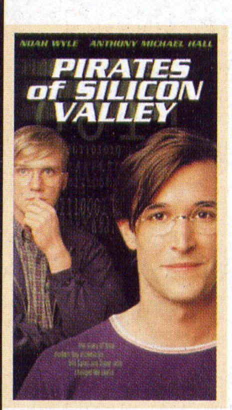
>> Final feliz

Woz ha abandonado un juego demasiado grande para él **y colabora con el distrito escolar de Los Gatos**, en California, donde ha armado a sus expensas laboratorios para los chicos de las escuelas medias, a los que dedica parte de su tiempo enseñándoles el uso del ordenador.

EN VIDEO

HISTORIA DE LOS PIRATAS DE SILICON VALLEY

Los exordios de Wozniak y Jobs (y los paralelos de Bill Gates y Steve Ballmer, fundadores de Microsoft) son brillantemente contados en el film "Piratas de Silicon Valley". La cinta distribuida por Warner Bross es difícil de encontrar, pero los comercios y sitios de alquiler más grandes pueden suministrarla sin problemas.



WOZCAM EN DIRECTO

En **www.woz.org**, Steve responde personalmente a cientos de emails respecto a la historia de Apple y de la informática en general. Además de esto, y de otras informaciones interesantes, se puede echar un vistazo al estudio de Steve pilotando la Wozcam, una webcam motorizada que se puede orientar a distancia con el propio navegador.

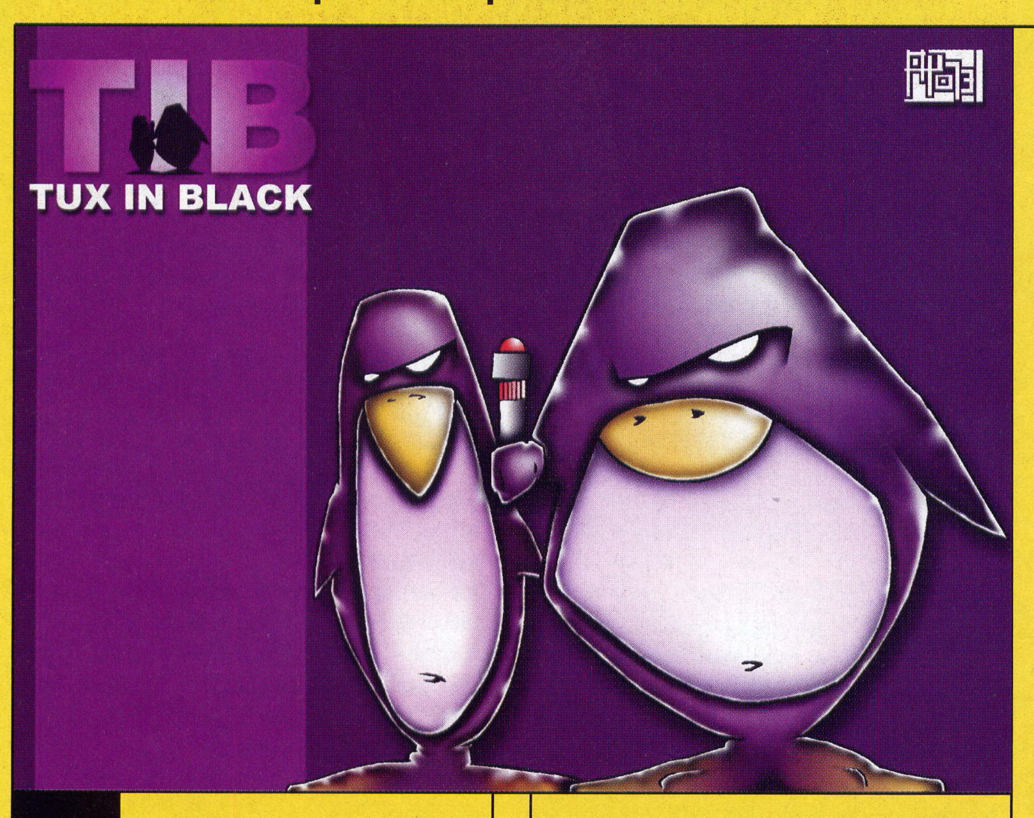


Apple I, el primer ordenador Apple, tenía un procesador 6502, 4 KBytes de memoria, podía usar un reproductor de casette como memoria de masa y se adaptaba a una decoración clásica: en los primeros ejemplares, la caja era íntegramente de madera.

PEQUEÑO DICCIONARIO PARA QUIEN VIAJA DE MS-DOS A LINUX

Primeros pasos en Linux

Si finalmente has decidido instalar una distribución Linux, probablemente te parecerá estar en un país extranjero del que no conoces la lengua. He aquí un diccionario útil para las operaciones fundamentales.



Para quien se acerca por primera vez a la fatídica "línea de comando" de Linux, (ya sea bash o cualquier otra), quizá procediendo del clásico MS-DOS, seguramente resultará agobiante, cuando no frustrante, el no conseguir realizar las operaciones más banales: copiar un archivo, crear un directorio y visualizar el contenido de un .txt resultan ser obstáculos casi insalvables frente a los que se sueltan insultos y golpes en el teclado.

En realidad, si bien posee una versatilidad y una complejidad netamente superiores al viejo DOS, la shell de Linux permite efectuar todas estas operaciones básicas de forma similar, añadiendo a menudo una cantidad de opciones que raramente se podían encontrar en la ya obsoleta -pero siempre útil- shell de Microsoft.

Vayamos pues a dar una ojeada más o menos profundizada todos los "fundamentos" indispensables en el uso de una shell UnixLike: la sintaxis y las opciones presentes en la brevísima guía que hay a continuación las puedes encontrar mediante un simple man [comando] directamente en tu línea de comando (además de otra información, no olvides que Linux es uno de los sistemas operativos mejor documentados del mundo).

Antes de iniciar, una obligada recomendación: a diferencia de MS-DOS, Linux distingue entre mayúsculas y minúsculas, por lo que los comandos y la operaciones deben ser insertados exactamente como se indica en el texto.

>> Listar el contenido de un directorio

Comando MS-Dos: dir
Sintaxis Bash/Linux: ls [opc.] [file...]
dir [file...]
vdir [file]

Se trata sin duda del comando más usado: a través de éste podremos visualizar en la pantalla en contenido de un directorio, y mediante el uso de una serie de parámetros y opciones podremos efectuar búsquedas sobre el nombre del archivo, etc.

Opciones:

-C lista los archivos ordenados verticalmente en columnas.

-F añade a cada nombre de directorio una '/', una '¦' a las FIFO y un "*" a los ejecutables.

-R lista recursivamente todos los subdirectorios encontrados.

-a incluye en el listado todos los archivos cuyo nombre empieza por ".".

-c usa la hora del último cambio de estado del archivo y la hora de la última modificación para ordenar (con -t) o para listar (con-l).

-d lista los directorios como los otros archivos y visualiza sus contenidos.

-i imprime el número de índice (inode) de cada archivo, a la izquierda del nombre.

-l escribe en una (única columna) los permisos del archivo, el número de enlaces (link) hacia él, el nombre del propietario del grupo, el tamaño (en bytes), el horario y el nombre. El horario mostrado es el de la última modificación; las opciones -c y -u seleccionan los otros dos horarios (último cambio de estado y último acceso). Para los archivos especiales de dispositivo, el campo





del tamaño se reemplaza por norma por el número mayor y menor del dispositivo.

-q imprime los caracteres no representables de un nombre de archivo como interrogantes (este puede ser el default en caso de output en el terminal).

-r invierte la dirección del orden.

-t ordena según el horario mostrado.

-u usa el horario de último acceso para ordenar (con -t) o listar (con -l).

-1 output sobre una columna única.

>> Copiar un archivo

Otro de los comandos más utilizados: su funcionamiento es simple, copia el contenido de un archivo en otro.

Comando MS-DOS: copy
Sintaxis Bash/Linux: cp [opciones] archivo recorrido
cp [opciones] file... directory

Opciones:

-f elimina los archivos de destino preexistentes, si es necesario (ver arriba)

-i pide confirmación antes de sobrescribir archivos de destino preexistentes; mejor usarla en las primeras pruebas antes de borrar archivos importantes.

-p conserva propietario, grupo, permisos (incluidos los bits setuid y setguid) fecha de última modificación y fecha del último acceso de los archivos originales.

-R copia los directorios recursivamente, adaptando el resultado en base al encuentro de objetos diversos de archivos ordinarios o directorios.

-r copia los directorios recursivamente, comportándose en modo no especificado con objetos diversos de archivos ordinarios o directorios.

>> Crear un directorio

Comando MS-DOS: md
Sintaxis Bash/Linux: mkdir [opc.] directory...

El comando permite crear un directorio en el que archivar datos de todo tipo. Los permisos heredados del directorios creado son normalmente los mismos del usuario que lo crea.

Opciones

-m, --mode Modo. Configura los permisos, que pueden ser simbólicos como en chmod, comando del que hablaremos en un próximo número, y usa los permisos predefinidos como punto de partida.

-p, --parents Crea cada directorio padre que falte. Por ejemplo, si te encuentras en un directorio vacío y quieres crear dos directorios, el uno dentro del otro, bastará escribir md /nuevodirectorio1/nuevodirectorio2 -p. En este caso, el directorio nuevodirectorio2 se creará en nuevodirectorio1. Si nuevodirectorio1 no existe, y no se usa la opción -p, el resultado será un error.

--verbose visualiza un mensaje de confirmación para cada directorio creado. Esto es útil especialmente junto con -p.

>> Mover o renombrar un archivo

Comando MS-DOS: m/move
Sintaxis Bash/Linux: mv [opc...] destinación surgente
mv [opciones...] salida... destino

Permite desplazar un archivo a otro, definiendo el nombre de la copia.

Si se copia un archivo con un nombre distinto del original pero en la misma posición, el resultado final será que el archivo será renombrado.

Opciones:

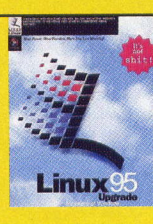
-f no pide confirmación.

-i pide confirmación cuando, en la posición de destino, existe un archivo con el mismo nombre (en el caso en el que se hayan usado tanto -f como -i, la última opción dada toma la preferencia).

>> Borrar un archivo (o un directorio)

Comando MdDos: del/rd/deltree
Sintaxis Bash/Linux: rm [opc.] file...

Obviamente, permite borrar un archivo del disco. Sin duda, se trata de un comando muy peligroso. A diferencia de la papelera de Windows, una shell Unix, no tiene una cestita en la que se pueden recuperar los archivos borrados por error. Antes de pulsar Intro, controla que hayas configurado correctamente cada opción.



Opciones:

-f No pide confirmación. No escribe mensajes de diagnóstico. No produce un estado de retorno de error si los únicos errores eran archivos inexistentes.

-i Pide confirmación (en el caso en que se hayan usado tanto -f como -i, la última opción dada tiene preferencia).

-r o -R Elimina árboles de directorios en modo recursivo. Esto significa que si estás en tu directorio Home y escribes rm -R borrarás con toda seguridad todos tus documentos.

>> Nuevas aventuras

Estos son los comandos fundamentales que te permitirán empezar a usar la shell. Existen muchos más comandos y programas: cat, vi, less y otros harán posible editar archivos o visualizar sus contenidos... Recuerda que para obtener documentación exhaustiva sobre cada uno de ellos es suficiente un man [comando]... Si en cambio no tienes idea de qué comando necesitas, pero sabes que te sirve, por ejemplo, para copiar un archivo, lo mejor es un "about copy" que te restituirá todas las referencias necesarias para obtener información más detallada sobre el tema que te interesa.

```
LS(1)                System General Commands Manual                LS(1)

NAME
     ls - list directory contents

SYNOPSIS
     ls [-ACFLRSTWacdfgiklnoqrstux1] [file ...]

DESCRIPTION
     For each operand that names a file of a type other than directory, ls
     displays its name as well as any requested, associated information.  For
     each operand that names a file of type directory, ls displays the names
     of files contained within that directory, as well as any requested, asso-
     ciated information.

     If no operands are given, the contents of the current directory are dis-
     played.  If more than one operand is given, non-directory operands are
     displayed first; directory and non-directory operands are sorted sepa-
     rately and in lexicographical order.

     The following options are available:

     -A      List all entries except for `.' and `..'.  Always set for the
             super-user.

     -C      Force multi-column output; this is the default when output is to
             a terminal.

/tmp/man.001287 (12%)
```

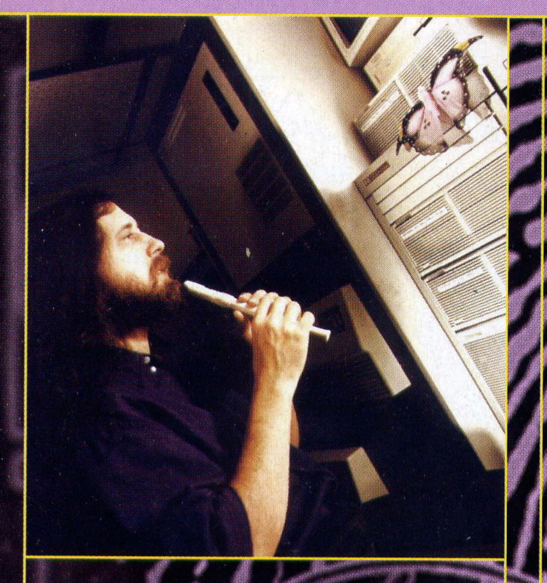
el manual del comando ls, obtenido escribiendo "man ls" (sin comillas) en la línea de comando. Pero en este caso se trata de la shell Tcsh de Mac OS X.

ENTREVISTA A RICHARD STALLMAN, EL PADRE DEL SOFTWARE LIBRE

Richard Stallman: entre software

Nos encontramos con él, después de su seminario sobre el

que ha respondido a muchas preguntas que habíamos preparado para él. Esta entrevista



Háblanos de la Free Software Foundation, y del "Free Software".

Muchos tienen las ideas confundidas en cuanto al software libre. En parte, a causa de la ambigüedad de la palabra inglesa "free", que significa "libre" o "gratuito". En la expresión "free software", la palabra "free" significa "libre" y no "gratuito". Los españoles deberíais sacar mejor partido a vuestra lengua, hablando de "Software Libre", y no del "Free Software".

¿Qué características tiene el software libre?

El software libre da a sus usuarios plena libertad. Pueden copiarlo, distribuirlo, leer su código fuente y modificarlo. Sólo tiene la obligación de redistribuir el software sin poner límites a la libertad de la que gozaba. (Nota: estos conceptos están expresados en términos legales en la licencia GNU Public License, que se encuentra en www.gnu.org/copyleft/gpl.html, y que acompaña al software libre. La GPL impide, por ejemplo, que un fabricante modifique el software libre e imponga un copyright).

Esta filosofía no se aplica solamente al software.

Diría que este es el nuevo desafío. Obviamente, cosas como el hardware no podrán ser libres por mucho tiempo aún. No es posible copiar el hardware, porque por ahora no existen tecnologías que puedan reproducirlo. A pesar de esto, no podemos basarnos solamente en las tecnologías de copia actuales, porque esta infravaloración de la tecnología es la principal responsable de las limitaciones de libertad que sufrimos hoy.

Explícanos por qué.

Hace tiempo no existían reglas que impidieran copiar los libros. Cualquiera podía copiar a mano un libro, como los amanuenses de la Edad Media. Con la llegada de las tecnologías de imprenta, los autores y los editores han pedido leyes que impidieran la replicación de un libro, afirmando que la ausencia de estas reglas habría desanimado la producción de nuevos libros. Visto el elevado coste de las máquinas de imprenta, para el gran público no era posible efectuar copias impresas de libros. De hecho, las personas estaban renunciando a una libertad que no habrían podido ejercer, y el "intercambio" entre libertad de copia y disponibilidad de nuevos libros parecía muy conveniente. Las leyes sobre copyright limitaban la libertad de los impresores, no la del gran público. Después, en la última mitad del siglo pasado, llegaron las fotocopiadoras, las grabadoras de casette, las grabadoras de vídeo, y por último las tecnologías de copia digital. Ahora la limitación de libertad es mucho más pesada para el común de las personas, y sería razonable negociar un nuevo contrato menos restrictivo.

¿Y en cambio?

En cambio, las leyes sobre el copyright son cada día más pesadas. La constitución americana contempla el copyright, pero por un tiempo determinado. Lo que pasa es que las grandes empresas que retienen los derechos promueven leyes que cada vez extienden más el tiempo de validez de la prohibición. Es el caso, por ejemplo, de lo que yo llamo la "Ley Mickey Mouse", con la que Disney ha prolongado retroactivamente por 20 años el copyright sobre la figura de Topolino, un personaje que ya debería ser de dominio público. Pero, gracias a la tecnología, los grandes han llegado al punto de no necesitar las leyes para imponer el copyright.

¿Por ejemplo?

Los contenidos digitales están protegidos con sistemas de criptografía y protección desde los accesos. Como es ilegal violar estos sistemas, es ilegal también copiar su contenido, si bien en teoría su circulación debería ser libre. Tomemos los e-Books, los libros electrónicos cifrados y protegidos por un password. De momento los e-Books están poco difundidos, y nadie se preocupa. Dentro de 20 o 30 años, el copyright de algunos e-Books podría caducar, pero la copia de estos e-Books seguiría siendo ilegal porque para copiarlos sería necesario engañar o violar la protección del software, un acto que está per se fuera de la ley.

El copyright se define también como "derechos de autor".

Nada más falso. La verdad es que los autores están entre las entidades más dañadas por los contratos de las casas discográficas, y muy a menudo no perciben nada por su propio tra-

libre y derechos civiles

tema "Copyright y Comunidad en la era de la Red", en la representa, por tanto, una síntesis de su intervención.

bajo. Las casas discográficas sólo reconocen una mínima parte de sus ganancias en un disco. Pero lo que pasa muy a menudo es que ni esta pequeña parte llega efectivamente a los autores, porque las casas discográficas retienen estas ganancias para compensar la inversión para la promoción del disco. A menudo estos términos se renegocian cuando caduca el contrato, pero el contrato prevé, por ejemplo, que el grupo o el autor deba realizar seis o siete discos antes de que el contrato caduque. Solamente los grupos más grandes y populares llegan a esta meta.

Pero hay quien dice que hay que garantizar a los autores una justa compensación.

El hecho de que un producto del intelecto sea "libre" no significa que deba ser gratuito. Nada impide que un CD de música "libre" se venda como una bella confección. Quizá se podría crear un sistema para hacer donaciones directamente a los autores saltándose las productoras. Descargo libremente un tema de la Red, me gusta y decido dar un dólar al autor, haciendo clic sobre un botón de mi PC. Pero soy libre de distribuirlo sin limitaciones.

Además del copyright, te has comprometido en otros frentes de la lucha por los derechos civiles. ¿Puedes hablarnos de ello?

Con la excusa del terrorismo, los gobiernos han empezado a atacar la libertad de los ciudadanos. En los años 80 ha despertado escándalo una ley del Sur de África que permitía a la policía encarcelar una persona durante 30 días sin necesidad de pruebas ni de procesos (a menudo, pasados los 30 días la persona era liberada y arrestada pocos minutos después). Con las leyes y los procedimientos impuestos después del 11 de septiembre, en los EE.UU. es posible encarcelar a una persona por un tiempo indefinido, sin proceso y sin pruebas, simplemente declarando que se trata de un "combatiente extranjero terrorista". La policía no tiene necesidad de probar esta afirmación. Sostengo que hoy el presidente Bush y el ministro de Justicia Ashcroft son las dos personas más peligrosas del mundo por lo que acontece a los derechos humanos.

Volviendo al software, ¿qué diferencia hay entre Software Libre y Open Source?

El movimiento del software open source "recomienda", pero no impone, dejar a los usuarios la libertad sobre el software. Esto significa que las empresas que hacen disponible el propio software como Open Source siguen manteniendo algunos derechos sobre el producto. El movimiento Open Source es menos radical. Por ejemplo, afirma que el software comercial es bueno, pero no es la solución óptima, mientras que los de la Free Software Foundation decimos que el software comercial representa el mal. En resumen, hay una cierta afinidad entre las dos corrientes, y las diferencias no superan el 1% de las posiciones.

¿Qué piensas de este encuentro?

Estoy verdaderamente electrizado por el entusiasmo de los participantes. Especialmente por el entusiasmo por los aspectos más políticos de la cuestión.

¿QUIÉN ES RMS?

Richard Stallman, o RMS como firma a menudo, nació en 1953 en Manhattan. En 1974 se licenció en Harvard, durante su vida académica, formó parte del equipo del laboratorio de Inteligencia Artificial del MIT, y trabajó en el desarrollo de sistemas operativos. En 1975 escribió el programa Emacs, popular editor de texto para Unix. En 1984 dejó la universidad para fundar el proyecto GNU con el objetivo de desarrollar el sistema operativo GNU (Gnu is Not Unix) del que hoy día Linux es una variante (y de hecho sería necesario llamarlo siempre GNU/Linux, y no sólo Linux, que es solamente el nombre del kernel). Además del desarrollo y la difusión del software libre, Richard está en primera línea de la batalla para la defensa de los derechos civiles en EE.UU. y en el mundo, especialmente los relativos a la libertad de expresión del pensamiento y al copyright.



Como de costumbre, al final de su intervención, RMS se puso una túnica y una aureola realizada con un disco para ordenador de 8" para representar San IGNUcio, y pidió al púbico que hiciera la profesión de fe de la iglesia de Emacs: "No tendrás otro OS fuera de GNU, y Linux es uno de sus kernel".



La FSF te necesita

Además de recoger donaciones que le permitan llevar adelante sus actividades, la Free Software Foundation necesita voluntarios que contribuyan a sus proyectos. En particular, se necesitan personas que tengan actualizado el directorio de software libre (**www.gnu.org/directory**), dedicando algunas horas a la semana. La información para participar se puede encontrar en **www.gnu.org/help/directory.html.**

CÓMO NACEN Y CÓMO SE DIFUNDEN LOS VIRUS

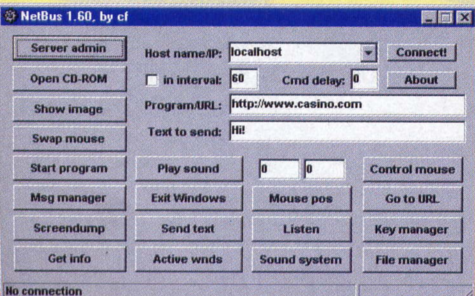
Virus: el fenómeno

Breve historia de uno de los fenómenos más devastadores del lado

El virus es un programa. El nombre VIRUS deriva del hecho que tales programas se auto reproducen y están obligados a pegarse a otro programa. En la práctica, la misma cosa que haría un virus biológico, que, para infectar, reproducirse y vivir en nuestro organismo, necesita una célula.
Los virus suelen estar escritos por hábiles programadores, pero **en la Red se encuentran aplicaciones que permiten, incluso a los novatos, crear un virus complejo con unos pocos clics.**
Algunos virus están escritos solamente por las ganas de ponerse a prueba del programador, para "ver si es capaz", o para demostrar su bravura al mundo. Otros no son más que una broma. A veces consisten en enviar un mensaje de protesta o de otro tipo. En realidad, muy pocos virus están escritos con el objetivo de hacer daño.

>> La historia de los virus informáticos

La historia de este fenómeno nace con el mismo inicio de la informática:
En 1959 tres programadores de Bell Laboratories desarrollaron "Core Wars", un juego en el que cada uno de los programadores escribía programas capaces de reproducirse, y los escondía en el ordenador. A una señal convenida, cada virus intentaba reproducirse y destruir a los otros. Al final vencía el que podía presumir de un mayor número de virus reproducidos, es decir, quien había creado el virus más potente. **En 1970 nace Creeper**. Se trata de un virus creado por Bob Thomas difundido en la red ARPAnet. El virus se presentaba escribiendo en pantalla "I'm Creeper, catch me if you can!". **En los años 80 nace el primer Caballo de Troya**. Un programador creó una versión de un famoso juego llamado Animal, que durante la ejecución se reproducía metiéndose en todos los sistemas conectados. El objetivo del programador era difundir un nuevo método de distribución del software llamado "Pervasive Release". Este tipo de programa tomó el nombre de "Caballo de Troya" para indicar que contenía en su interior un agente infeccioso.



NetBus permite tomar el control total del equipo en el que se instala, y una vez en su interior, se maneja a través del control de la versión server del programa.

En 1985 en Italia nace Ping Pong, un virus que hacía aparecer en la pantalla una simpática pelotita que rebotaba produciendo daños. Ping Pong procedía del Politécnico de Turín. En el mismo instituto universitario se desarrolló la utilidad Devirus, que individuaba el código Ping Pong y lo eliminaba.
En 1986 sale a la luz Brain, un virus que infectaba el sector de boot del disquette floppy. Brain fue desarrollado en Pakistán por dos hermanos, Basit y Amjad. Brain no tenía un código dañino, sino que se limitaba a introducirse en todos los disquetes insertados en el lector de un ordenador infectado y modificaba la etiqueta con el texto "(c) Brain".
En 1990 la complejidad de los virus hizo un paso adelante. Se crearon virus definidos como polimorfos. Un hacker conocido como Dark Avenger distribuyó el Mutation Engine, un programa que permitía a cualquiera crear virus polimorfos.

La llegada de Windows 95 marcó un giro de 180 grados. Empezaron a aparecer los primeros virus capaces de sacar partido de las debilidades de este sistema operativo.
Una verdadera revolución llegó cuando se presentó una amenaza prácticamente inesperada: los virus macro. La primera infección de este tipo que entró en libre circulación fue **Word.Concept**, que usaba el lenguaje de programación de Microsoft Word. Así como el mismo lenguaje de scripting se usa en otros programas de Microsoft, el primero Outlook y su versión gratuita Outlook Express, han empezado a difundirse virus específicos para el correo electrónico, que usan estos programas como vehículo de contagio. Han nacido, por tanto, virus con una velocidad y una amplitud de difusión nunca vistas: **Melissa, I Love You y muchos otros**.

Troyanos y Backdoor

La tipología de virus que más amenaza nuestra privacidad es la de los caballos de Troya, o una subtipología llamada Bakdoor Trojan. Están constituidos por una aplicación de tipo cliente y por un servidor (que reside en el ordenador infectado).
La parte del servidor puede insertarse en



de la Destrucción

oscuro del hacking, con una descripción de las tipologías de virus principales.

el interior de cualquier archivo ejecutable y representa el archivo que se difundirá mediante e-mail o a través de cualquier software. Una vez activada la aplicación del servidor, **quien tiene el cliente y las claves de acceso puede tomar el control completo de la máquina-servidor, y efectuar operaciones de transferencia de archivos, control de la red, búsqueda de passwords, apertura de la unidad de CD y docenas de operaciones.**



Heurística: tecnología antivirus que tiene bajo control algunos síntomas típicos de la presencia de un virus, com por ejemplo modificaciones no previstas en el tamaño de un archivo.

Los backdoor más conocidos son sin duda Back Orifice y NetBus.
Back Orifice es un backdoor proyectado para Windows que permite tomar el control de una máquina. Los intrusos pueden acceder al servidor de BO usando una interfaz textual para Unix o un cliente gráfico para Windows. El servidor de BO permite a los intrusos ejecutar comandos, leer archivos y ejecutar transferencias de archivos desde tu PC y hacia él, modificar el registro, iniciar y parar los procesos y muchos otros trucos. **NetBus permite, a través de un simple panel de control, desarrollar las mismas funciones que BO y muchas otras.** Entre ellas, la apertura del micrófono de tu ordenador, transformándolo en un espía que escucha lo que estás diciendo.

>> Cómo defenderse

Para disminuir el riesgo de infección hace falta **instalar un antivirus y actualizarlo constantemente** (al menos mensualmente). ¡Tener un antivirus no actualizado equivale a no tenerlo! Es oportuno controlar la presencia de virus en el propio PC, controlando cualquier CD o floppy de procedencia sospechosa antes de ejecutar cualquier archivo en ellos. **Es importante no ejecutar nunca programas de origen desconocido**. Controlar siempre todos los archivos que se meten en el sistema, porque **la difusión de los virus viene sobretodo con el intercambio de archivos entre amigos o por e-mail**. El correo electrónico es uno de los principales medios de difusión de virus: basta abrir el archivo infectado adjunto a un mensaje para ser contagiado. controla siempre los archivos adjuntos con un programa antivirus. En particular, controla los archivos con las extensiones: exe, dll, com, sys, vbx, pif, scr, ocx, vbs y los documentos que pueden contener macros: doc, xls, dot, xla. Un método para defenderse de programas de Backdoor Trojan es **instalar un buen programa de detección y actualizarlo frecuentemente**. Este programa debería ser ayudado por un **cortafuegos, que controla rigurosamente todos los programas que intentan acceder a Internet** y señala quien intenta entrar en nuestro ordenador. Obviamente, el sistema más seguro de todos es aparcar el ordenador y usar la máquina de escribir...

Nazareno S.

TIPOLOGÍAS DE VIRUS

Existen varios tipos de virus informáticos, catalogables en base a cómo se comportan, sobreviven y se autotransmiten. He aquí una lista:

BOOT SECTOR VIRUS: infectan la parte de un floppy o disco duro que contiene información necesaria para el inicio del sistema. La difusión se da generalmente cuando se inicia un ordenador con un floppy infectado.

FILE VIRUS: son virus que infectan archivos de programas (con extensiones .exe, .com, etc.) y se reproducen a cada inicio del programa infectado.

MACRO VIRUS: es el tipo de virus más difundido. En la práctica es un programa escrito en Visual Basic (VBA o Visual Basic for Applications).

MULTIPARTITE VIRUS: para difundirse usa una combinación de técnicas. El tipo más común usa el método de trabajo de un virus de boot y de archivo.

POLYMORPHIC VIRUS: es un virus que muta cada vez que se reproduce.

STEALTH VIRUS: usa varios trucos para esconderse y esquivar los softwares antivirus. En general son virus que infectan el DOS. Existen muchas variantes de este virus:

MBR STEALTH: este virus infecta el MBR "master boot record" salvando una copia del MBR original que sustituye a la infectada cuando un antivirus va a controlar la sección de master boot record.

CLEAN ON-THE-FLY: este virus intercepta todas las operaciones de lectura sobre los archivos. Si un antivirus lee un archivo infectado el virus intercepta la operación de lectura y limpia el archivo devolviéndolo normal al control. Una vez acabada la operación, el virus reinfecta el archivo.

TROJAN VIRUS: es un programa que contiene en su interior un subcódigo dañino que se activa al determinarse ciertas condiciones.

ZOO VIRUS: son virus que viven solamente en laboratorios de investigación porque no pueden difundirse.

IN-THE-WILD VIRUS: son virus que viven en estado salvaje, es decir, han esquivado el control y están actualmente en circulación.

SE DIFUNDE CADA VEZ MÁS LA RED SIN HILOS. PERO ¿GARANTIZA LA SEGURIDAD NECESARIA?

Seguridad en el éter

Con el protocolo 802-11b es posible cortar los cables Ethernet y navegar en red a alta velocidad. Pero ¿hasta qué punto resulta este sistema seguro? Analicemos el estándar, el protocolo y los gusanos que ya se han descubierto.

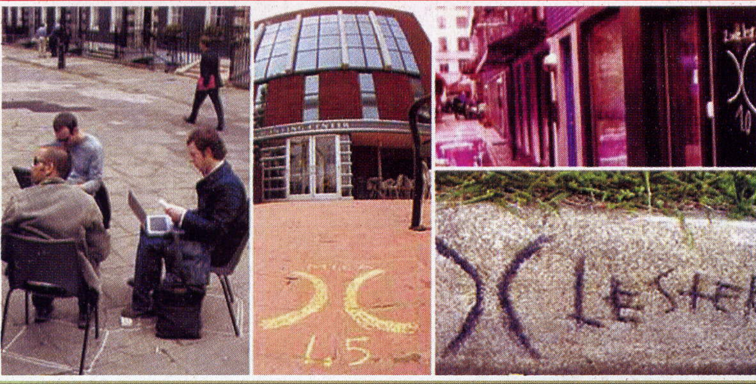
En estos últimos tiempos, gracias a las ventajosas ofertas presentadas por numerosos proveedores de Internet, se está difundiendo cada vez más el nuevo protocolo de red IEEE 802-11b. Conocido públicamente como Wireless Internet, o Wi-Fi, permite conectar con una red Ethernet sin hilos dos o más ordenadores personales con una velocidad máxima de 11 megabits por segundo.

>> Internet sin hilos

En la base de esta tecnología de red wireless se usan tarjetas de red, normalmente conectadas a un puerto USB o PcCard (Pcmcia), en este último caso instalable en los ordenadores desktop mediante el convertidor PCI adecuado. Gracias a estas tarjetas es posible superar eventuales obstáculos arquitectónicos sin tener que agujerear muros para tirar cables, aunque el uso prevalente se hace en ordenadores portátiles. En muchos de los nuevos laptop de gama alta, además, ya está presente el soporte nativo integrado en su interior. Los MacIntosh, en cambio, tienen un spot de tipo propietario al que se puede conectar una tarjeta Airport (el nombre comercial dado por Apple a este aparato), pero pueden utilizar tarjetas Pc-Card o PCI de otras marcas.

El protocolo, codificado por el ente internacional IEEE (www.ieee.org), **prevé dos configuraciones predefinidas Ad Hoc e Infrastructure.** En el primer caso permite conectar **dos ordenadores entre ellos, en modalidad peer-2-peer.** La modalidad Infrastructure, más compleja, **favorece la creación de subredes conectadas a la red fija a través de un Access Point**, dispositivo de acceso que se pone conceptualmente como vía media entre un hub y un router. Entre sus finciones, además de gestionar la conexión física entre las dos antenas, generalmente integra la posibilidad de proporcionar direcciones IP de modo dinámico, gracias a un servidor DHCP. Access



Algunos símbolos trazados por los War Driver para señalar la presencia de redes wireless accesibles.

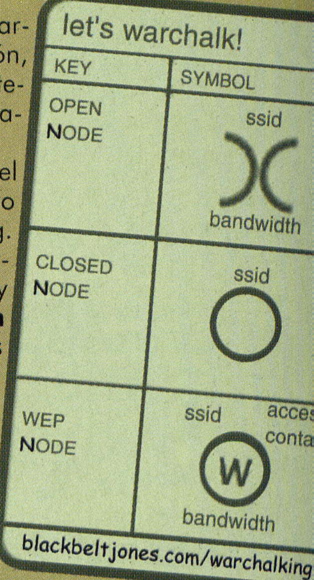
El argot de los war-drivers

¿Cómo reconocer si en una zona hay una red Wireless Ethernet no protegida? Entre los war-drivers se ha difundido una moda, tomada de las costumbres de las logias secretas del 1800: marcar con yeso en un muro o en el suelo un símbolo oportuno, aparentemente sin sentido, pero que otro war-driver puede reconocer. Los símbolos más usados son dos semicírculos verticales opuestos, con un nombre arriba y un número abajo indicando la banda disponible: esto significa un nudo abierto. Como alternativa, encontramos un círculo con un nombre escrito encima: en este caso, el nudo está cerrado. Si en el interior del círculo hay una W, significa que el nudo encontrado está protegido por el protocolo Wep.

Point siempre gestiona la configuración eventual de seguridad de la red.

>> Redes desprotegidas

Si por un lado las ventajas de un sistema completamente sin hilos son la total movilidad y la independencia de un lugar físico, por el otro existe el problema de que las ondas de radio no están "canalizadas" en un flujo privilegiado, sino que se difunden en el aire como gigantescas bolas electromagnéticas. Por tanto, nace el problema que **cualquiera, con una tarjeta de red conforme al protocolo u otros dispositivos de hardware, puede conectarse a la red si ésta no está oportunamente protegida.** El protocolo prevé un sistema para el cifrado de datos, llamado Wep, pero dada su complejidad de gestión no está siempre activado por los administradores, y deja las redes de muchas empresas abiertas a la posibilidad de conectarse sin ningún tipo de autenticación, simplemente "paseando" por el exterior de la sede provistos de ordenadores portátiles.



Está muy difundida, sobretodo en el extranjero, y es reciente en nuestro país, la práctica del War-driving. ¿En qué consiste? Se va con un portátil, sniffer y mapa de la ciudad y **se viaja en coche (o incluso en helicóptero) a través de las calles de una metrópolis a la búsqueda de puntos de acceso de radio.** Una vez encontrados, se intenta obtener una dirección IP del servidor DHCP, siempre que la conexión no esté protegida; también se puede intentar descubrir la clave de cifrado, operación que se ha demostrado que no es imposible, sino relativamente simple si se ejecuta con las herramientas adecuadas. Los war-drivers acostumbran a señalar en las paredes o aceras símbolos específicos que permiten a otra gente conectarse en red.

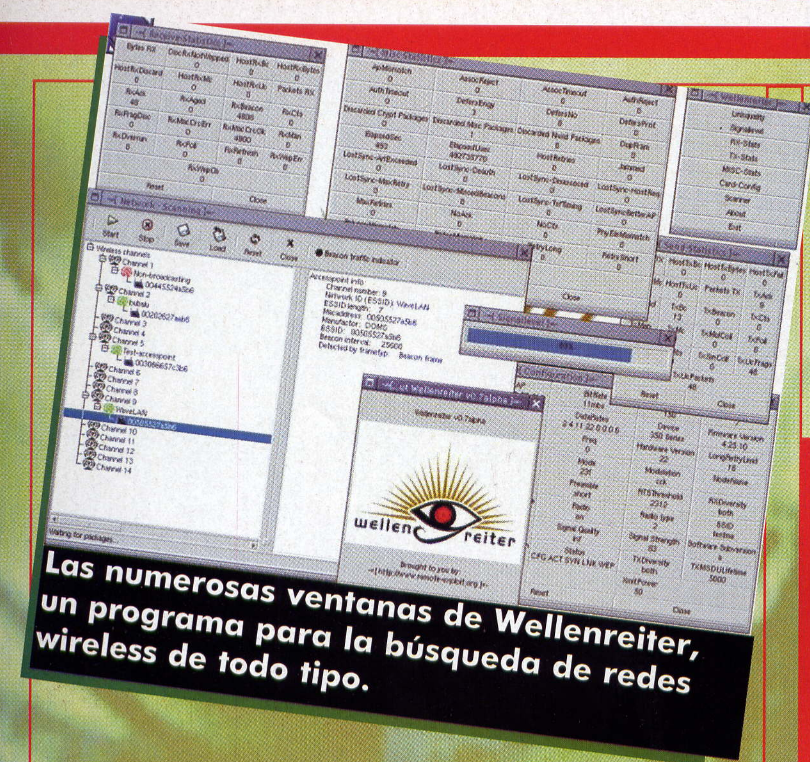
La defensa de la red

Si bien no se puede evitar la instalación de una red lo sin hilos, pero se desea hacerla lo más segura posible, pueden utilizar algunos programas creados expresamente.

S-Lan
http://slan.sourceforge.net
S-Lan, o Secure Local Area Network, es un proyecto op source que intenta garantizar una completa seguridad bilidad en las comunicaciones entre redes wireless y relativas LAN locales, o Internet. Su principal difer respecto al Wep reside en la creación de claves temp dotadas de vida muy breve y constantemente actualiza software está disponible para Windows y Linux.

Black Alchemy's Fake AP
http://www.blackalchemy.to/Projects/fakeap/fake-ap
Como se dice en la home page, si tener un access po positivo, tener millares puede hacer la vida muy di los war-drivers. Con este programa es posible gener cacofonía de señales, escondiendo así el verdadero point de usuarios no deseados.

Open Node Closed Node WEP Node



Las numerosas ventanas de Wellenreiter, un programa para la búsqueda de redes wireless de todo tipo.

>> Redes protegidas

Veamos ahora cómo se estructura la protección contenida en las especificaciones del protocolo 802.11b. **El sistema de protección se llama Wep, acrónimo de Wired Equivalent Privacy,** que debería hacer imposibles las intercepciones entre las comunicaciones de radio. Usa el algoritmo RC4 en modalidad sincrónica. Se basa en un sistema de cifrado con dos claves, una pública (llamada Initialization Vector, de 24 bits) y una privada, inicialmente codificada con una longitud de 40 bits, sucesivamente aumentados a 128 bits, cuando la ley americana de exportación de técnicas criptográficas lo permitió. Usando un XOR sobre el XOR original de los paquetes enviados **es posible remontar al Initialization Vector y descodificar todas las comunicaciones protegidas por esta clave.** La longitud de 24 bits del Initialization Vector permite la creación de un número relativamente limitado de códigos de cifrado, que con el otro no deben ni siquiera cambiar en cada transmisión, según el estándar: monitorizando por un cierto tiempo una red wireless es posible crear una tabla que contenga todas las posibles claves de descriptación, utilizándolas para interceptar los datos e introducirse en la red. Existen algunos programas (ver cuadro) específicamente creados para forzar el sistema Wep y permitir accesos no autorizados.

>> Cómo protegerse

Llegados a este punto, ¿qué se puede hacer? **Si estás proyectando la construcción de una red wireless en tu empresa o en casa, ten en cuenta que la seguridad no estará garantizada al 100%** (¿cuándo lo está?) y que irá proyectada en el mejor de los modos **autenticando las direcciones de hardware (Mac Adress) en los nics o configurando reglas adecuadas con los cortafuegos. Como alternativa, se puede orientar en la red wireless un canal VPN (Virtual Private Network) cifrado**, obteniendo así un nivel de seguridad comparable al de una red cableada incluso si por desgracia de este modo se pierde algo en términos de eficiencia y prestaciones.

Francisco F.

Wi-Fi Cracker

Una pequeña relación de programas que podrían ser usados para efectuar el acceso a redes wireless desprotegidas, o incluso protegidas por el sistema de seguridad Wep.

802.11B NETWORK DISCOVERY TOOLS

`http://sourceforge.net/projects/wavelan-tools/`

Se trata de un programa gráfico para Linux que busca redes Wi-Fi usando el hardware del portátil. Incluye la posibilidad de memorizar las coordenadas usando un sistema GPS compatible Nmea conectado al puerto serie.

WEPCRACK

`http://wepcrack.sourceforge.net`

Programa opensource de texto estudiado para descubrir, utilizando el método descrito por Fluhrer, Mantin y Shamir, la clave de cifrado del sistema Wep.

AIRSNORT

`http://airsnort.shmoo.com`

AirSnort es otro software para Linux útil para la recuperación de la clave de cifrado de las Wireless Lan. Monitoriza pasivamente las transmisiones, intentando descodificar el password, en cuanto recibe un número suficiente de paquetes.

BSD-AIRTOOLS

`www.dachb0den.com/projects/bsd-airtools.html`

Software para sistemas operativos basados en BSD, que consiste en un completo set de programas para monitorizar la red de radio 802-11b. Permite crackear el protocolo Wep y buscar Access Point públicos.

WALLENREITER

`www.remote-exploit.org`

Wellenreiter es un programa gráfico para la búsqueda de redes wireless, señalando Access Point y sistemas ad-hoc. Soporta la gestión de tarjetas construidas por Prism2, Lucent y Cisco. Usando un sistema GPS permite memorizar las coordenadas geográficas de acceso a la red. Entre sus particularidades está la posibilidad de funcionar también en sistemas Linux/BSD a baja definición gráfica, como por ejemplo un PDA de la serie IPaq.

KISMET

`www.kismetwireless.net`

Kismet es un sniffer de red 802.11b. Permite buscar las más difundidas tipologías de tarjetas de red y sus protocolos relativos. Una de sus funciones crea un dibujo de las redes reconocidas, calculando la posible dimensión y adaptándolo a los mapas previamente insertados.

UN TROYANO HOY DÍA SUPERADO PERO AÚN EN CIRCULACIÓN

IDENTIFICATION ORDER NO. 10
October 10th, 2002

WANTED

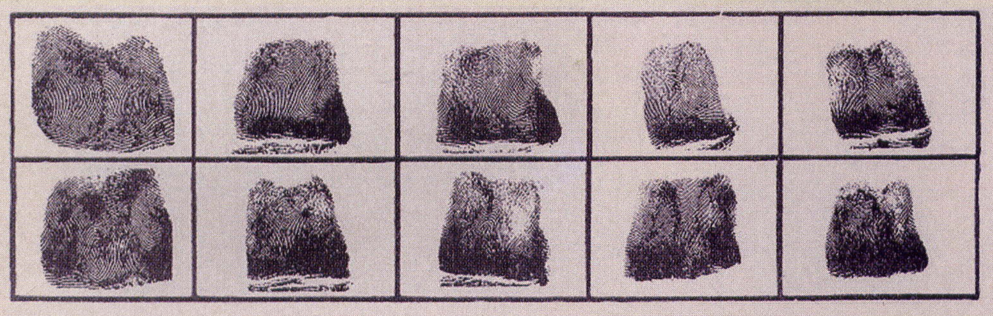
DIVISION OF INVESTIGATION H.J. DEPARTMENT OF NET

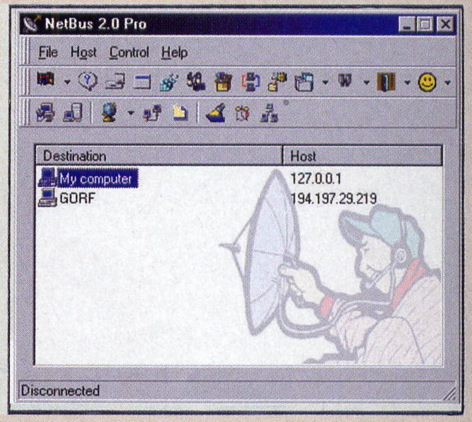
BARCELONA - ES.

Fingerprint Classification

16 0 5 U 001 20
I 17 U 001

NAME: NetBus
TYPE: Trojan
ALIAS: NetBus.153, NetBus.160, NetBus.170
DATE OF BIRTH: Marzo 1998
AUTOR: Carl-Fredrik Neikter





Acciones cumplidas:

Según la versión, NetBus puede efectuar muchas acciones diversas. Entre estas las más comunes son:

Server admin: modifica la configuración del servidor (eliminar el servidor, cerrarlo o configurar las direcciones IP que pueden entrar en el ordenador).
Start program: ejecuta una aplicación.
Screendump: captura la pantalla.
Get info: muestra información sobre el PC.
Port redirect: captura los datos enviados a un puerto y los desvía a una cierta dirección IP o puerto.
App redirect: direcciona un programa cualquiera a un cierto puerto del PC.
Listen: ejecuta un keylog de todos los datos que la víctima inserta por teclado.
Control mouse: para controlar el ratón de la víctima.
Go to url: abre una ventana con un determinado sitio Internet.
Key manager: lee los passwords desde el disco y desde la memoria.
File manager: permite descargar, enviar y borrar archivos.

Medios de contagio:

Estar infectado por NetBus significa haber descargado y ejecutado de alguna manera el Servidor de Troyano en el propio ordenador. El Servidor debería ser reconocido por los antivirus pero el lamer de turno podría usar varios trucos: el archivo tiene la extensión .exe típica de los ejecutables, pero podrías encontrarlo como .scr (de hecho, los salvapantallas son propiamente ejecutables). Además, podría usar un programa tipo WPack32 para asociar el ejecutable con otros archivos (imágenes, textos, etc.) de modo que se ejecuten cuando la víctima abre la fotografía o el texto.

Signos particulares:

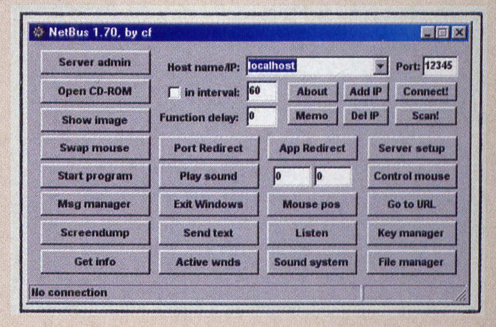
Los Servidores son frecuentemente archivos con extensión 'exe' que se instalan en directorios ya muy llenos (tipo Windows o Windows\System) con nombres similares a archivos del sistema e iconos poco evidentes. Se configuran para partir en cada inicio de ordenador modificando el archivo System.ini, la Tarjeta de Ejecución Automática, y sobre todo algunas claves del Registro de Configuración. Una vez iniciado, el Servidor pone en escucha un cierto puerto a la espera de recibir órdenes del Cliente. A veces, el acceso al Servidor está protegido por password. Contrariamente a Back Orifice, NetBus no crea procesos visibles desde el exterior, por lo que resulta difícil interceptarlo. A diferencia de las primeras versiones, el Servidor de la versión 2.0 se llama NBSvr.exe, usa el puerto predeterminado 20034 y crea su llamada (en el Registro de Configuración) a la ruta HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Instrucciones para la detención:

Para verificar si el propio ordenador está infectado por NetBus se pueden usar varios métodos:

- el Servidor de NetBus emplea para el arranque, al iniciar el PC, una llamada que se crea en el Registro de Configuración de Windows. Verifica, mediante Regedit, si se ejecutan automáticamente rutas, archivos o programas "desconocidos" (elección más aconsejada aunque más arriesgada) en: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) se inician aplicaciones desconocidas. En este caso, borra la clave y reinicia el ordenador y borra el archivo del servidor que se encuentra en el directorio indicado en la clave del registro que has eliminado.

N.B. Antes de hacer modificaciones decisivas con SysEdir y Regedit, haz una copia de los archivos a modificar; para un ojo inexperto las claves necesarias para el inicio y el correcto funcionamiento del PC pueden



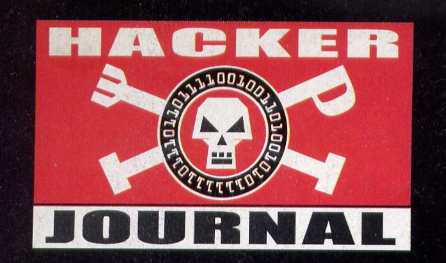
ser confundidas con nuestro "sospechoso".

- para identificar una infección genérica por troyano existe un método universal: iniciar desde el viejo DOS el programa 'Netstat' que señala todos los puertos abiertos o en escucha de tu ordenador.
- como alternativa se puede emplear un software como "The Cleaner 3" o "Trojan First Aid Kit 4" (www.sofotex.com/download/software/1743.html).

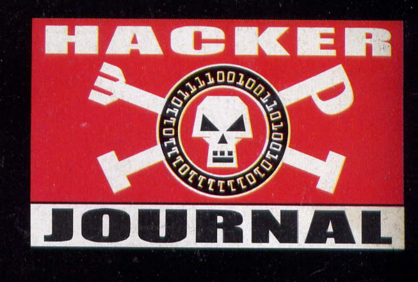
Más información:

www.hackfix.org/netbusfix/
www.nwinternet.com/pchelp/nb/netbus.htm

{RoSwEIL}



Guestbook



Las últimas firmas registradas en nuestro libro de visitas

Hola amigos. Enhorabuena por los 3 numeros de vuestra revista y por esta pagina. Kisiera saber como puedo conseguir vuestro nº2 ya ke donde vivo no se llego a vender. el nº1 y el nº3 si ke los tengo pero el 2 me falta. Espero ke os pongais en contacto conmigo para solucionar mi problemilla. Gracias. Un saludo a tod@s ([Chipiron+) • El nº 3 es el 1º que compro y me ha gustado mucho, a pesar de que soy un novatillo y hay cosas que se me escapan, pero todo se andará. Pr favor decidma cómo puedo conseguir los nº 1 y 2 y si hay manera de suscribirse, pues donde yo vivo, será difícil de conseguir. Gracias. (Diego) • Por fín una revista con contenidos interesantes... No decepcionarnos! (webBoss) • Hola!ante todo felicitar el buen trabajo ke haceis,pero os propongo a mejorar la redacción de algunos artículos como ¿kien se hace a GSM? en el ke no explicais con toa claridad el proceso de transformacion del movil en 1 scanner....Saludos de parte de la A.E.C.P1 (HuNk) • Soys la caña,seguid asi ([DF] Vincent Phoenix) • Saludo a todos y felicitar a los creadores de 'hacker journal' pues, por lo que he visto, empieza a estar bastante interesante. Aunque me encantaría conseguir la primera entrega.. Venga, me largo buena y mala gente.. ;P Hasta la próxima! (DtorBill) • muy bueno adelante los felicito. A mi la pag www.negone.com me acusa penalmente de ataque informatico sera una honeyweb o yo sere muy tonto (el_celta) • Wenas a tos!!!! me encanta esta revista. esxo k sigais asi xk estais exos una makinas i k esta web crezca con la ayuda de todos. saludos (Kali_Q) • Quisiera saber si esta operativa la, pagina si se actualiza, si es asi decirmelo i donde puedo conseguir la revista en murcia (_F3R_) • Me kompro todas las hacker journals ke salen a la venta y realmente me gustan muxo...))) (Lord Sauron) • Hola! hace tiempo estaba buscando una revista de este tipo y hoy por casualidad la he encontrado , lo q ocurre es que ya va por el Nº 3 q es el q he comprado pero el 1º y el 2º no los tenian ¿Es posible hacerse con esos 2 numeros atrasados? Un saludo la revista es de puta madre y estoy muy interesado en aprender a hacer todas estas "cosikas". (Principiante) • El nivel es muy elemental animo continar asi (tirk) • que pagina de puta madre. quiero aprender a programar si alguien me puede mandar informacion de como aprender que contacte com migo por e-mail (adrian) • El nivel es muy elemental (básico), aunk para uno que empieze no esta mal. A Kuidarse. (diabolic) • soys la mejkor revista que ahi pr 1amig dic k sois uns btaiaspor k dicen k 1 hacker no puede sacar 1 revist por k es ilegal (alberto) • Hola a todos, he estado esperando todo este tiempo para poder tener el 2o número de la revista. Para mi la mejor de hack (a la mierda ARROBA). YO SOY DE HACKERS JOURNAL!!! (KiKe) • Hoy he visto la revista en un kiosko, y digo... vaya flipada de revista, pero la he comprado xD y la he estado leiendo y es mas interesante de lo que pensaba. A ver si continuais metiendo buen contenido que eso es lo mas dificl, buenos contenidos en cada numero :P Un saludo. (MorK)



Nos vemos en el próximo número

¡Resistid sin nosotros!

www.hacker-journal.com